Al-Nahrain Journal of Science
ANJS, Vol.24 (1), March, 2021, pp. 45-56

Forged Copy-Move Recognition Using Convolutional Neural Network

Ayat Fadhel Homady Sewan* and Mohammed Sahib Mahdi Altaei

Department of Computers Science, Collage of Science, Al-Nahrain University, Baghdad, Iraq

Article's Information

Received:
26.10.2020
Accepted:
24.01.2021
Published:
13.03.2021

Keywords:
Copy-move
CNN
Image forgery recognition
Buster net
Digital forensics

Abstract

Due to the extreme robust image editing techniques, digital images are subject to multiple manipulations and decreased costs for digital camera and smart phones. Therefore, image credibility is becoming questionable, specifically when images have strong value, such as news report and insurance claims in a crime court. Therefore, image forensic methods test the integrity of the images by applying various highly technical methods set out in the literature. The present work deals with one important research module is the recognition of forged part that applied on copy move forgery images. Two datasets MICC-F2000 and CoMoFoD are used, these datasets are usually adopted in the field of interest. The module concerned with recognizing which is the source image portion and which is the target one of that already detected. Thus, the two detected tampered parts of the image are recognized the original one from them, the other is then referred as forged or tampered part. The proposed module used the buster net of three neural networks that basically adopted the principle of training by using Convolution Neural Network (CNN) to extract the most important features in the images. The first and second networks are parallel working to detect and identify areas that have been tampered with, and then display them through two masks. While the last network classifier takes a copy of these two catchers to decide which is the source image portion from the two detected ones. The achieved recognition results were about F-score 98.98% even if the forged area is rotated or scaled or both of them. Also, the recognition results of the forged image part was 98% when using images do not contributed in the training phase, which refers to that the proposed module is more confident and reliable.

DOI: 10.22401/ANJS.24.1.08

*Corresponding author: progayat@gmail.com

1. Introduction

The technical advancements and the internet's convenience make people can easily access fascinating multimedia from the internet and change or manipulate it [5]. Since images are stronger than hundreds of words, the World Wide Web (WWW) includes a huge number of digital images that are used to communicate effectively [6]. Since images are also used in various important areas like evidence of crime, medical imaging, banking, studies into the environment and weather, military information, and several other applications. Image authentication has been demanded due to the need to pass images between various unguaranteed communication methods **[7]**.

2. Copy Move Forgery

The copy-move is a special form of forgery that includes cloning part of an image and then pasting the copied part into the same image is the copy-move forgery image. Therefore, in network society, image forensics correlated with copy-move forgery detection is becoming increasingly prevalent [5]. Because the copied part comes from the same image, it will be compatible with the rest of the image with its major properties, such as noise, brightness and texture, making it more difficult for professionals to identify and detect the alteration [8]. Figure 1 shows a Facebook photo of a group of Prime Minister Najib Tun Razak supporters is marked a copy-move forgery one because it is very clear that the crowd has been duplicated to look bigger [3].

It is also very important to explore image manipulation, as the image could be utilized as valid evidence, during forensic science as well as in other areas [9]. There were many traditional techniques to forgery detection, most of which include block-based and key points-based extraction of features and matching techniques [10]. Deep learning methods have now been introduced for overcoming the issue of forgery digital images. Nevertheless, most methods are focused with supervised learning. While there are a number of instances classified, it is easier for training the model through supervised learning. In order to overcome the issues for training set, they usually replace training sets using an adjacent datasets or using artificial

images. When these datasets assess same model, it results in a large decrease in efficiency. This occurs caused by a change in form, contents, or appearance distributed of different dataset. In these situations, domains adapting are required to learn the distribution change. In this work, they showed which manipulation of pictures through various fields can be identified through filed adaptation. Researchers take full advantage of Convolution Neural Networks (CNNs) to see the distinctive features of genuine as well as forgery images [11].

Figure 1. Fake photo by copy-move forgery [3].

3. Related Works and Contribution

A lot of studies for the recognition of forgeries. They differ in several ways, such as the content the image, that process used, and even the constraints of applications. The effectiveness of using forgery images detection focused on a deep learning using CNNs is explored in the following section:

3.1 Related works

Detection of cloning forgery has received a lot of attention. In order to gain more effective approaches to support wide applications, methods were developed. Most significant studies are mentioned with detail as in following:

In 2018, Bin Yang, Xingming Sun, Honglei Guo [12] focused on passive forgery detection of tampered images using copy move technique known as Copy Move Forgery Detection (CMFD). A CMFD technique consisting of oriented Features from Accelerated Segment Test and rotated Binary Robust Independent Elementary Features (Oriented FAST and rotated BRIEF)or (ORB) as the feature extraction method and 2 Nearest Neighbors (2NN) with Hierarchical Agglomerative Clustering (HAC) as the feature matching method is proposed. Evaluation of the proposed CMFD technique was performed on images that underwent various geometrical attacks. With the proposed technique, an overall accuracy rate of 84.33 % and 82.79 % are obtained for evaluation carried out with images from the MICC-F600 and MICC-F2000 databases. Forgery detection achieved True Positive Rate of more than 91% for tampered images with object translation, different degree of rotation and enlargement.

In 2019, Younis Abdalla, Tariq Iqbal M. and Mohamed Shehata [13] suggested a new scheme built on neural networks and deep learning, focusing on the architectural method of the convolution neural networks (CNN) to improve the identification of copy-move forgeries. A CNN architecture that integrates pre-processing layers to offer satisfactory results is used in the proposed approach. The present study, features 15 layers in total: one each of input and output classification layers, one Soft Max layer, one max-pooling layer, two average-pooling layer. Furthermore, the potential for different copy-move forgery strategies to use this model is clarified. The auto resizing layer was modified to inject unrestricted size images and output modified union dataset size to 64×64×3 to fit with the input to the first convolutional layer. Learning training was implemented with different image batch sizes: 64, 100 and 265, with the same preliminary learning rate of 10−3. The various batch normalization sizes used (e.g., 64, 100 and 256) and 7 epochs. The first one was constructed by Christlein, consisting of 48 base images and 87 copied with a total of 1392 copy-move forged images. The second database, MICC-F600, was introduced by Amerini et al. [16, 39] with 400 images. The dataset was divided into 70 % training data and 30% testing data. The experiment results show that the overall accuracy of validation is 90%, with a fixed iteration limit. While the accuracy of the proposed method(FRI) exceeded 98% because we used three networks that depended on the principle of CNN, not only one network, that is, it trained more and determined the size of the input images (256,265,3), a number of 250 cycles, 30 packages, and a learning level (0.01). The proposed method also managed to make a decision. Which of the two regions is the source of the copy, whichever is the target copy. In 2019, Mehta V., Jaiswal A. K. and Srivastava R. [10] proposed copy-move forgery detection (CMFD) technique relies on DCT and ORB feature extraction and distance-based clustering approach. Extracted DCT features are matched based on Euclidean distance. Extracted key-points using ORB are matched using k-NN procedure based on Hamming distances. To enhance the accuracy, a distance depend clustering method is used to eliminate false matches. For research on (CoMoFoD) small datasets, the proposed technique is applied. The accuracy of the results reached about 96%. Experimental findings show which method is effective in finding copy move areas and are also stable in illumination and variance alteration, noise increase, geometrizing updates such as scale. Because reduce false matches and refine the resulting image a breadth-first search-based clustering technique is implemented.

In 2020, Dhivya1 S., Sangeetha J. and Sudhakar B. [14] proposed a technique used Speed Up Robust (SURF) features extraction, also particular objects are identified using the support vector machine (SVM). The image features are coordinated to find the similar portions in order to reduce the computational unpredictability and to improve the accuracy of false recognition. In proposed

methodology evaluate on real-time images captured from various mobile phones such as Moto 5 g plus, Samsung S7 edge, and Micromax canvas knight 2. Once copy-move was done, several changes were made to an image. That modified image shown in the results are extracted from a dataset. The testing outcomes show that the suggested method can achieve remarkable and successful result. The accuracy ranged between [80-96] according to the difference in the data. Moto 5 g plus got the best accuracy, while the Micromax canvas knight 2 got the lowest. In 2020, Chen H., Yang X. and Lyu Y. [15]. Main point based detection is identified as being successful in detecting forgery of copy/cloning motion (CMFD)). In order to identify tampered areas, an effective CMFD approach is suggested by clustering SIFT key points and looking for similar neighborhoods. Based on color and size, the key points are clustered, grouped up into multiple small units and separately matched. This greatly reduces computation time induced by a high dimension of SIFT when matching. Finally, a new position technique is built for evaluating the related neighborhood of matching pair by two likeness measure in addition to accurately determine a tampered parts at pixels-level, and to iteratively label the tampered regions in pixels. The experiments are conducted on the tampered images of three public domain benchmark databases: GRIP, Dataset (D0) and FAU which all consist of tampered images and corresponding ground truth images. The experimental results showed a forgery acceptable only detection F1-score is 98.07 %.

4. Contribution

The contribution of the present work impact the determination of the original part from those two parts were referred to as forged. This issue was ignored and has not being discussed in previous studies, current study focused on just such issue. In addition, the task of specifying the place of a cloning in the image is more interesting and involves a thorough analysis of the content of the images. According to our accounts, this task requires the use of the deep learning for determining the forged part found in the image. The approach used will be compared and verified with current state-of-the-art methods in terms of performance, robust, time-complexity matching, detecting reliability and forgery position accuracy that are beneficial for verifying the authenticity and integrity of digital images.

5. Proposed FIR Method

The general structure of the proposed forgery image recognition (FIR) is depicted in Figure 2. Where, the main objective of the proposed FIR is to recognize the forged part in the image using CNN for additional image description by adopting two ways: the manipulation net and similarity net. Similarity branch is work to compute the similarity between the detected original (source) and forged (target)image parts, and stored these similarities in a binary mask. Where manipulation branch is work detected only forgery (target) copy. As a results, two masks are determined, each enclose a tampered image region. The two resulted masks are input into fusion branch for recognizing the original one from that forged input segments. The decision given by the fusion net mask will ensure the location of the two parts compared parts of the image, and then determine which of them is the original one. The proposed method involves the use of different colored bands to strength the feature extraction and achieving efficient descriptors from target image. The following sections explain more details about each stage in the proposed FIR method.

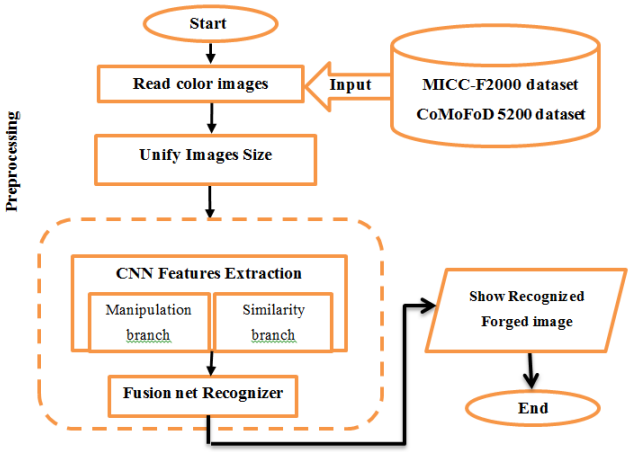


Figure 2. Block diagram of the proposed CMFD method.

5.1 Image preprocessing

Image preprocessing step includes unifying the size of the input image, which is required from the CNN to make the plane of the CNN layers is unified with same architecture for all input image. In order to implements such step. It is not a requirement that the height (H) of the image be the same as its width(W), but the entry must be standardized to get maps of features of equal size to be compared between them. In the proposed method, a size of 256 height (H) and width (W) was adopted because it was the most appropriate in terms of recognition accuracy and time.

5.2 Buster net

Buster net is designed to be a complete system for recognizing the original part of the image. It contains three parts within, they are: manipulation net, similarity net and fusion net. Each net operates according to the CNN principles. The CNN based manipulation net is used to ensure the forged parts detected in the first stage, The CNN based similarity net is used to ensure both the forged and authentic parts detected in the same stage, while the fusion net is used to recognize the original one of them and regarding the remaining ones of the label to be forged [16]. The inputs of the Buster net are a set of authentic color image, forgery image, mask of each forgery image. While, the output is a mask (Ground troth) of the manipulation

(forged) part of the image and its location in the source and target image. The manipulation net is training the CNN on the forged parts of the image that candidate to be forged (Manipulated) parts. This established net depends on input the detected forged segments of the image into a manipulation net that contain 25 layers within to extract significant features and then store these features in a feature map. A **feature map** is obtained for each filter in the layer by repeated application of the filter across sub regions of the complete image, i.e., convolving the filter with the input image, adding a bias term, and then applying an activation function as equation (1). After that apply rectified linear activation function or ReLU for short is a piecewise linear function that will output the input directly if it is positive, otherwise, it will output zero as equation (2) [17] and also displays the manipulation part in a binary mask.

$$p[f] = \sum_{ij} w_j * x_i + b \quad (1)$$

$$\mathrm{Re}(p) = \max(0, p) \quad (2)$$

where, p convolution process apply image, * is convolution operation, x value of image, i index for image, w value of filter, j index of filter (kernel), b is bias parameter which is used to adjust the output along with the weighted sum of the inputs to the neuron, Re is Relue activation function, p is feature map [18].

Whereas, the similarity net is training the CNN to find the similar parts of the image that candidate to be original (Similar) parts that resulted from the first stage. Also, it depends on input the detected forged segments of the image into similarity net that contain 29 layers within to extract features and then store these features in a feature maps as equations (1)-(2). The considered parameters in the CNN that taken in account are given in Algorithm 1 present the main steps of the buster net recognition stage. The fusion module takes inputs from both branches (paths) of the Mask Decoder features and considers these two branches together and allows the final prediction of the CMFD. The outcomes of our evaluation show that Buster Net outperforms state-of-the-art techniques by a big margin, and is also strong against different established CMFD attacks. More significantly, Buster Net has the powerful advantage of differentiating source/target copies over any current CMFD solutions. This is the ideal skill of forensic specialists [16]. Soft max is a mathematical function that converts a vector of numbers into a vector of probabilities, where the probabilities of each value are proportional to the relative scale of each value in the vector as formula [19]:

$$f(x) = \frac{e^{x_i}}{\sum_j^c e^{x_j}} \quad (3)$$

The cross-entropy function, through its logarithm, allows the network to asses such small errors (loss) and work to eliminate them. Say, the desired output value is 1, but what you currently have is 0.000001. Through some optimization, you are able to make that rise up to 0.001, Here's the formula for cross-entropy is [20]:

$$CE = -\sum_i^c t_i \log(f(x_i)) \quad (4)$$

where $f(x)$ is values of soft max function, CE is value of loss by apply cross-entropy [20].

Algorithm 1. Buster net stages for source image part recognition.

Input	Img**:** Set of authentic and forgery color image. M^f**:** Mask of forged parts in the image. M^o **:** Mask of original parts in the image.
Output	M_m^x**:** Manipulation mask localize target (forgery) part in forgery image. M_s^x**:** Similarity mask localize cloned regions. M_c^x**:** Fusion mask predicts target (forgery) part(s) in the image. $\mathrm{Img}^{\mathrm{final}}$**:** Image recognition source and target copy.
Begin	**Step 1:** Send input image into branches manipulation net and similarity net, in parallel. **Step 2:** Kernel sizes at (3,3), (5,5), (7,7) and (11,11). **Step 3:** In manipulation net CNN feature extract which essentially convert an input image (Img) for set of feature of interest $p[t] = (f_1, f_2, \cdot, f_t)$ and store in feature map by apply steps as following: • Convolution//layer performs several convolutions by using filters to get linear activation as equation (1). • Activation function//such (relue) as detector stage used to set the weights on the neuron to pass the positive values and to convert the negative to zeros by the following equation (2). • Pooling//replace a certain location with a summary statistic of the nearby output. • Fully connected layer // to convert feature map into array to easy compute. • Features matching which measure the likeness between features (f_i and f_j) for each $f_i, f_j \in p[t]$, apply binary mask decoder for manipulation nets to predict area of manipulation in image, M_m^x. **Step 4:** In similarity net CNN features extract, which essentially convert an input images (img) for group feature of interest $p[t] = (f_1, f_2, \ldots, f_t)$ and store in feature map by apply steps as following: • Convolution//layer performs several convolutions by using filters to get linear activation as equation (1).

	• Activation function//such (Relue) as detector stage as equation (2). • Percentile Pooling//choose only similar features. • Fully connected layer//to convert feature map into array to easy compute. • Calculate features similarity by Self-Correlation module. • Apply binary mask decoder for manipulation nets to predict area of manipulation in image, M_s^x. **Step 5:** Fusion net pull input for the Mask Decoder features from both branches (M_m^x, M_s^x). • Concatenate feature f. • Fuse features via the BN-Inception with parameters set 3 at [1, 3, 5] filter size. • Prophecy the three type CMFD masks by convolution using one filter with size (3×3). • Using a soft max activation function, fusion net predict mask, M_c^x, distinguish background (blue color), copy of source (green color), and copy of target classes mask (red color) as equation (3). • Compute loss by apply cross entropy function as equation (4). **Step 6:** Image detect border for source and target copy, X^{final}.
End	

Table 1, which can be determine in advance by trial and error for preparing the model for the training process. More details about input/output packet for each part of Buster net based recognition are given in the following subsections:

Table 1. Parameters of the CNN and their expected values.

Parameter	Value
Optimizer	Adam (lr=0.01)
Pooling	max pooling
Epochs	250
Batch size	30

6. Results and Discussion

Two well-known datasets are used to test and compare the performance of different forgery detection methods, they are: MICC-F2000 and CoMoFoD. These forgery images in these datasets are constructed by cloning parts of the image and pasting them into the same image For the purpose of challenging the credibility of the image. Many types of transformation have been applied to fake images, such as rotation (90˚, 180˚ angle), translation, scaling or combination of them. These datasets are composed of images that have different sizes. firstly, The MICC-F2000 data set consists of an images have different sizes, dataset are JPEG images format [4]. Figure 3 illustrates some dataset samples of the tampered images of MICC-F2000 dataset. Whereas, the CoMoFoD dataset contains 5200 tested images, each image is found with two samples: tampered and original. These 5200 images are found in small image category of 512×512 dimensions, each with JPEG and PNG image format. Also, these images are found without any transformation, but there is a colored mask indicates the original and forged regions, in which the black refers to the background, while the colored mask refers to the areas that have been forged. For detection assessment, the dual (binary) mask is useful where the dark mask refers to the background, and the white mask refers to the forged and original regions. Where, the forged image is the image with copied region(s). Figure 4 illustrates some dataset samples of the tampered images of CoMoFoD dataset [2]. The following subsections presents more explanation about the results of each stage of the proposed FIR method.

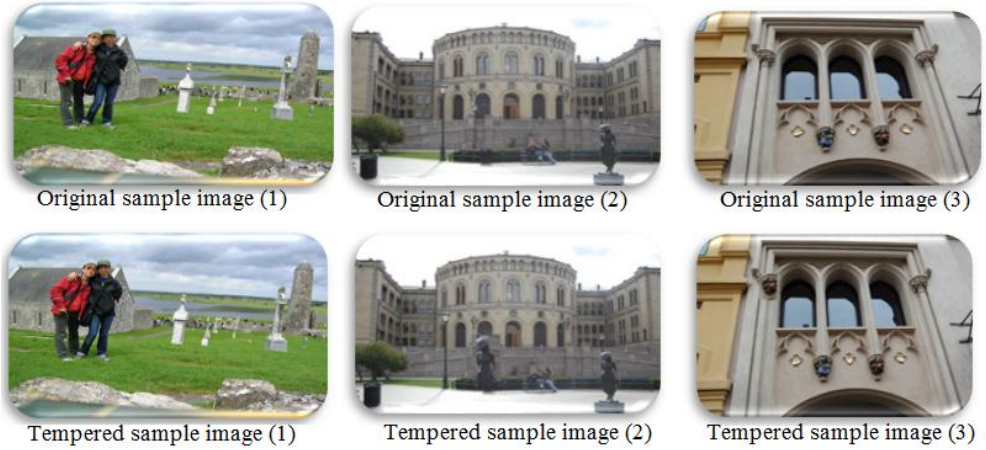


Figure 3. Sample images of MICC-f2000 dataset, images in upper row are authentic while images in lower row are its forged ones [4].

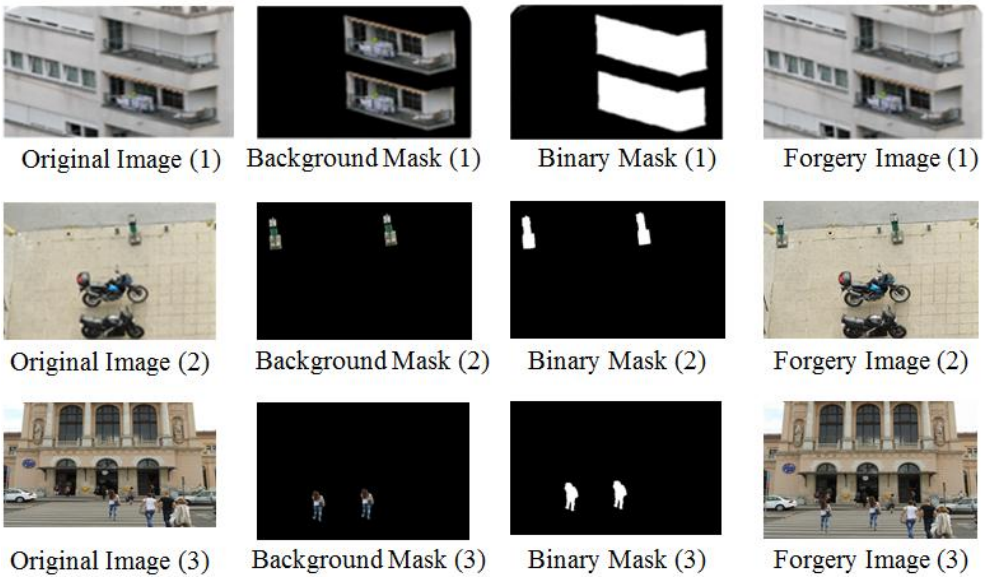
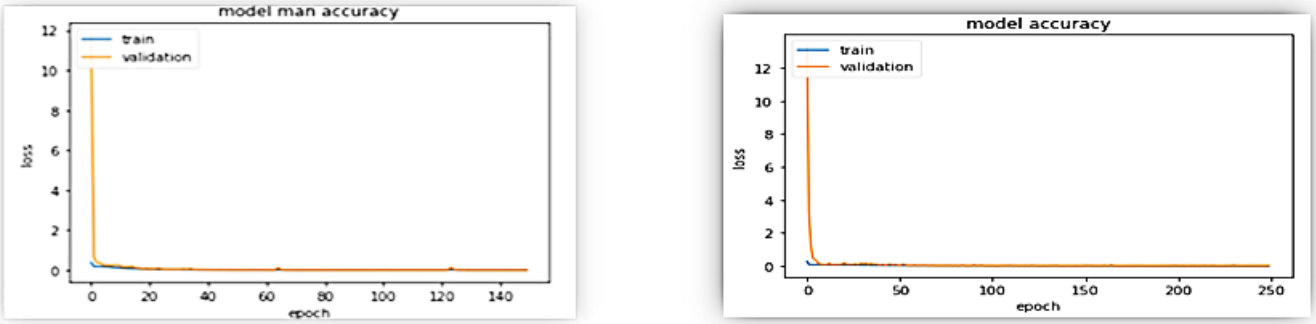


Figure 4. Sample images of CoMoFoD dataset, they are: original image, black mask, binary mask, and forged image sequentially [2].

6.1 Manipulation detection behavior

The main aim of manipulation net is to segment manipulated region. This region is determine by a mask and then extracts its features using CNN from the input image. The features map is then up sampled by apply max pooling to be as same as the real images dimension by masks de-coder, then the dual/binary classifier is applied for fulfilling the extra role (in other words creating a handling masks). The dataset was divided into 80 % for training and 20% for testing. The result of training model loss manipulated branch with two data set, as illustrated in Figure 5. It is shown that both the training and validation of the manipulation start with high rate of loss, and then the loss of them is decay into acceptable rate with increasing the number of epochs till reaching zero loss when epochs became greater than 76. This indicates acceptable behavior for the manipulation net toward the training and recognition with more runs. With CoMoFoD, 150 were used because the data contained one holder for the fake and the original part, while in MICC-F2000 the data required more than 150 cycles because it contained two masks so need more training.



(a) Model accuracy of CoMoFoD with 150 epoch

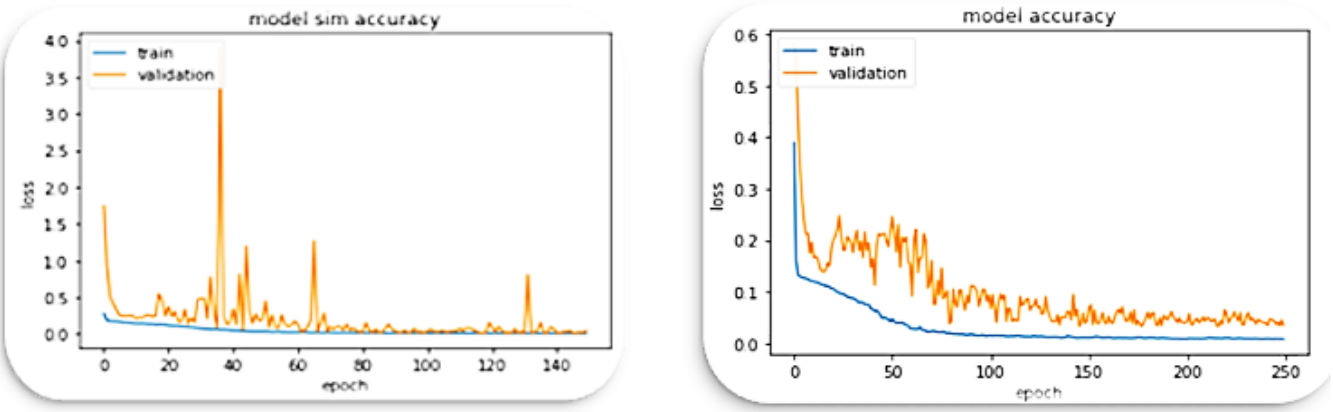
(b) Model accuracy of MICC-F2000 with 250 epoch

Figure 5. Result of model loss manipulated branch two data set.

6.2 Similarity Detection Behavior

Like manipulation detection branch, similarity detection section begins on features represent through the CNN features extracting. The result of training model loss similarity branch with two data set, as illustrated in Figure 6. It is noticeable that both the training and validation of the similarity branch start with higher rate of loss, and then the loss of them is decay into acceptable rate with increasing the number of epochs till reaching a value is approaches zero when epochs became greater than 80. This indicates acceptable behavior for the similarity net toward the training and recognition with more runs. Also, it is shown that the behavior of the similarity through implementing the validation mode is greatly fluctuated about the line of its progress; this is due to late accrued in the training phase. Also, such fluctuation refers to the great amount of training needed to make the similarity branch is able to recognize the tampered part in the image and apply

of two source and target mask in the similarity net when using the MICC-F2000 data Set. After 80 epochs, the fluctuations decreased and the mean value of them remains across zero. It is expected that the loss (which refers to the error in the similarity detection) became zero with more and more training for additional images have same specification of the used dataset.

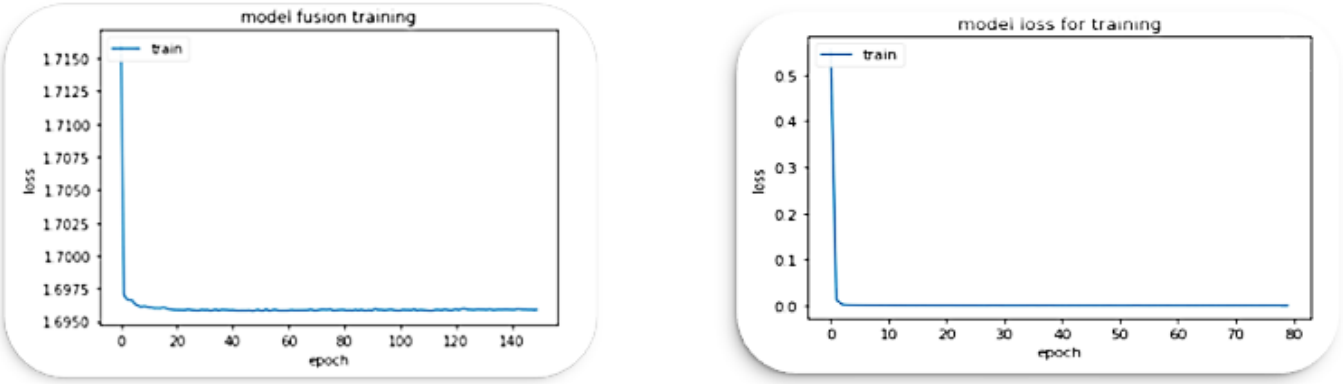


(a) Model accuracy of CoMoFoD with 150 epoch (b) Model accuracy of MICC-F2000 with 250 epoch

Figure 6. Result of model loss similarity branch two dataset.

6.3 Fusion detection behavior

The auto-detection with a deep learning method is necessary to determine a forged image. This is especially important for distinguishing an original source image from a forged one. The resulted training model loss of the fusion branch with two data set for source/target copy detection in buster net is illustrated in Figure 7. It is shown that the loss in the fusion performance began with a great value and then fast decay toward an acceptable level of error. With increasing the number of epochs, the loss decreases till reaching a rate approaches zero. Also, there is a little fluctuation was appeared in the behavior of the fusion net was coming from the similarity net, such little fluctuation not affect the recognition decision due to it represents less amount of error can impact the true recognition decision. The most important fact is the stability of the error (loss) mean upon zero value with increasing epoch through the considered limits. It is shown that the total loss ratio of the buster net was about 1.692 %, which was calculated by testing all sample images found in the used dataset.



(a) Model accuracy of CoMoFoD with 150 epoch (b) Model accuracy of MICC-F2000 with 80 epoch

Figure 7. Result of model loss fusion branch two data set.

In Fusion Detection Results, Figure 8 shows resulted forged parts in sample images belong to the dataset for source/target detection using fusion net, in which the first column represents the used sample images of resolution 256×256, the second column is the ground truth, and the third column localize the source/target copy in the original image. In order to verify the abilities of the descriptors used, fusion net classifier is checked several times depend on the features determined. In the Table 2 show the averages recognition ratings of 10 run for randomly-selected 20 different sample images located in the datasets each run. The first column refers to the number of run, the second column refer to the recognition score of the fusion net classifier. When using the convolution features in the

fusion net classifier. The average recognition rate (μ) is about 98.514 % and stander deviation (δ) is 0.419475, Calculated by Equation No. (5), meaning the acceptable and stability performance of the output of the classifier based on convolution features. This will serve the CNN training and recognition stages efficiently.

$$\delta = \sqrt{\frac{1}{n-1}} \sum_{i=1}^{n} (x_i - \mu)^2 \quad (5)$$

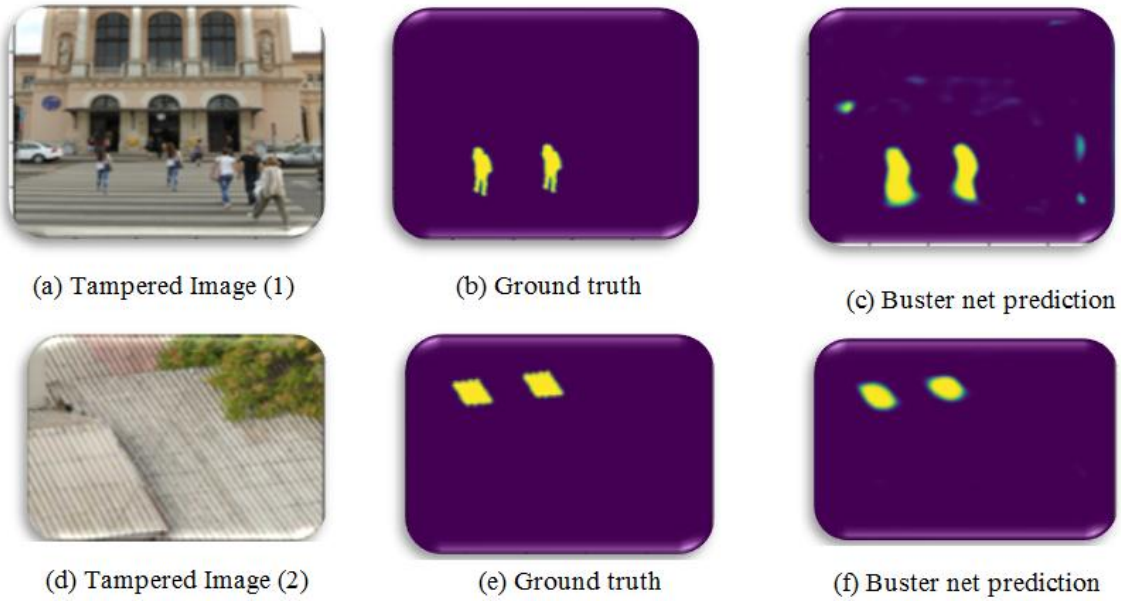


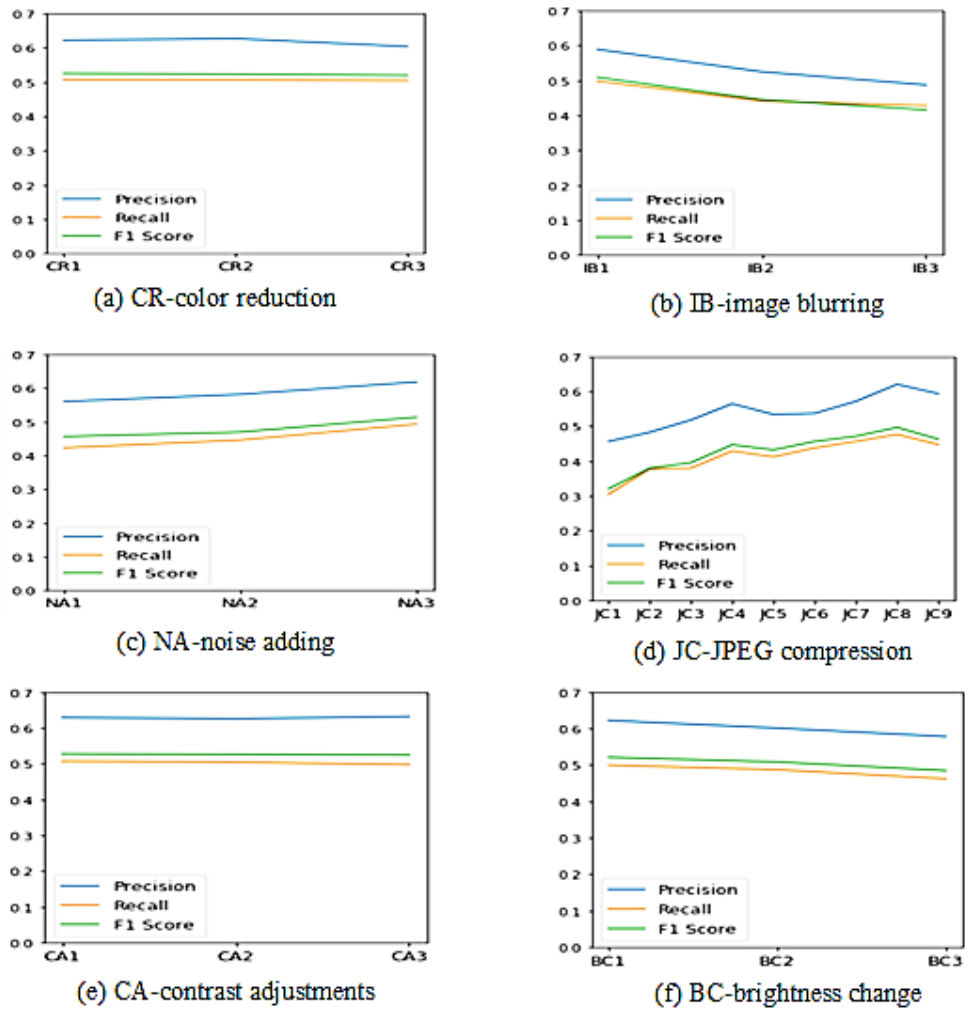
Figure 8. Results of detection source/target in image by Fusion net.

Table 2. On twenty randomly selected forged image samples, an average recognition value of ten runs each is applied.

Runs	Rec. Score % with Buster net
1	98.01
2	98.01
3	98.02
4	98.1
5	98.65
6	98.8
7	98.85
8	98.9
9	98.9
10	98.9
μ	98.514
δ	0.419475

For further tests, the proposed forgery detection method has been tested on another set of same CoMoFoD dataset that contains 5000 forged images found in the CoMoFoD (10400) datasets. This data set contain a mixture of images that contain geometric transformations after the copy move process, such as rotation, translate, scale and combination. This dataset is originally divided into six groups, they are: this dataset is originally divided into six groups, they are ('JC' JPE- compressing, 'IB' image-blurring, 'NA' Adding-noise,' BC' brightness-changes (low, top), such as (0.01, 0.95),' CR' color-reduce, intensities levels for every color canal,' CA'-contrasts-adjustment, (low,top) such as (0.01, 0.95)).

The proposed forgery detection method was applied on each group mentioned before three times, each one on one third (sub group) of the whole group. The forgery detection results of applying the proposed method on these six types of the used dataset are listed in Figure 9, while the performance measures (Precision, Recall, and F-Score) are shown in Figure 11. High precision score indicates that the learning annotator generated correct annotations. Also, low recall score indicates that the machine learning annotator success to create useful annotations. The measured average processing time for FID implementation was (3-4) hours. The success to detect and recognize the forged portion in the sample image reflects the high efficiency of the proposed method to be applied on different forgery image for purpose of detection. For each image, we extracted a separate F-score because it had a different post processing, as shown in Figure 4.10.



(a) CR-color reduction (b) IB-image blurring

(c) NA-noise adding (d) JC-JPEG compression

(e) CA-contrast adjustments (f) BC-brightness change

Figure 9. Behaviors of the performance measures of six groups images.

image_num	precision	recall	fscore
JC4_0	0.31	0.23	0.26
JC4_1	0.75	0.72	0.73
JC4_2	0.75	0.5	0.6
JC4_3	0.0	0.0	0.0
JC4_4	0.93	0.38	0.54
JC4_5	0.52	0.99	0.68
JC4_6	0.0	0.0	0.0
JC4_7	0.0	0.0	0.0
JC4_8	0.86	0.91	0.88
JC4_9	0.91	0.88	0.89
JC4_10	0.0	0.0	0.0
JC4_11	0.0	0.0	0.0
JC4_12	0.68	0.75	0.71
JC4_13	0.78	0.81	0.79
JC4_14	0.67	0.64	0.65
JC4_15	0.56	0.05	0.1
JC4_16	0.66	0.9	0.76
JC4_17	0.95	0.89	0.92
JC4_18	0.88	0.83	0.86
JC4_19	0.69	0.38	0.49
JC4_20	0.05	0.1	0.07
JC4_21	0.0	0.0	0.0
JC4_22	1.0	0.01	0.02
JC4_23	0.73	0.6	0.66
JC4_24	0.0	0.0	0.0
JC4_25	0.75	0.65	0.7

Figure 10. Sample results for each image of detection Fusion net.

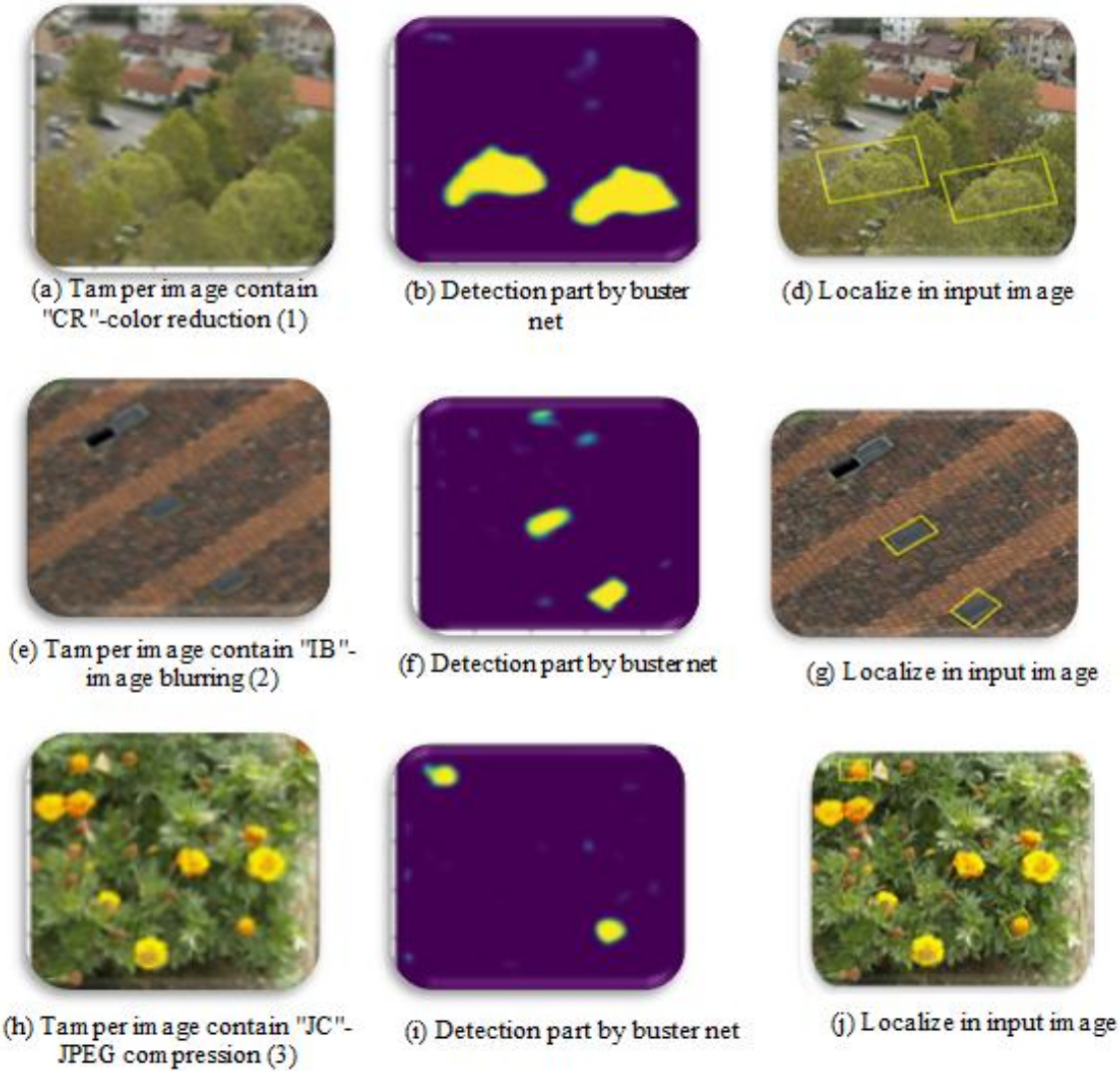


Figure 11. Detection and localization results for sample tampering images under post-processing attacks with F-score > 0.5.

7. FIR Results Evaluation

Our goal in this paper is not only to detect, but rather to recognize which of the two is the original (source copy) and which is forgery (target move). For this reason, it was intended to improve the process of identifying the original and the fogery. The evaluation includes two dataset; the first concerned with increasing the number of epochs up to 250 cycles. While the second is concerned with using another dataset, which is MICC-2000. This dataset contains two masks; one mask is used for man-net and another mask is used for the sim-net separately. Some original and tampered images used in the testing are illustrated in Figures 12. The evaluation gave acceptable results are compatible to that given from the recognition test based on buster net.

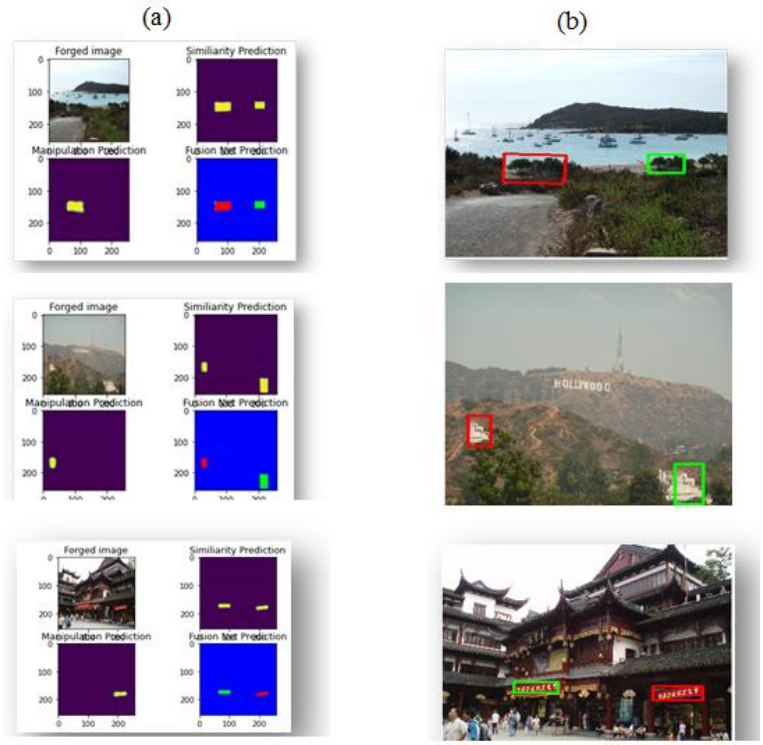


Figure 12. The detection and localize results for some tampering images. (a) Detection part; identified the original (source) part as green color and the forgery (target) as red color, (b) Localization parts.

8. Conclusions

Throughout the implementation, both the training and validation of the manipulation start with high rate of loss, and then the loss of them is decay into acceptable rate with increasing the number of epochs till reaching zero loss when epochs became greater than 76. Both the training and validation of the similarity branch start with higher rate of loss, and then the loss of them is decay into acceptable rate with increasing the number of epochs till reaching a value is approaches zero when epochs became greater than 80. The behavior of the similarity through implementing the validation mode is greatly fluctuated about the line of its progress; this is due to late accrued in the training phase. The loss in the fusion performance began with a great value and then fast decay toward an acceptable level of error. With increasing the number of epochs, the loss decreases till reaching a rate approaches zero.Total loss ratio of the buster net was about 1.692 %, which is a little and acceptable ratio. The average (μ) recognition score is about 98.514% with a variation amount of about δ=±0.419475, which indicates the high efficiency and stability of the classifier performance based on just convolutional features. Processing time for FRI implemented in a Google Colab platform was about (12) hours.

References

[1] Singh, R., Oberoi A. and Goel N., "Copy move forgery detection on digital images", International Journal of Computer Applications, 98(9), 2014.

[2] Tralic, D., et al., "CoMoFoD-New database for copy-move forgery detection", in Proceedings ELMAR-2013, IEEE, 2013.

[3] Abdel-Basset M., et al., "2-Levels of clustering strategy to detect and locate copy-move forgery in digital images", Multimedia Tools and Applications, 79(7), 5419-5437, 2020.

[4] Amerini I., et al., "A sift-based forensic method for copy–move attack detection and transformation recovery", IEEE transactions on information forensics and security, 6(3), 1099-1110, 2011.

[5] Huang H. Y. and Ciou A. J., "Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation", EURASIP Journal on Image and Video Processing, 2019(1), p. 68, 2019.

[6] Fadl S. M., Semary N. A. and Hadhoud M. M., "Fan search for image copy-move forgery detection", in International Conference on Advanced Machine Learning Technologies and Applications, Springer, 2014.

[7] Elaskily M. A., et al., "Two stages object recognition based copy-move forgery detection algorithm", Multimedia Tools and Applications, 78(11), 15353-15373, 2019.

[8] Sridevi M., Mala C. and Sandeep S., "Copy-move image forgery detection in a parallel environment", in Proceedings of Im age and Signal Processing, Cisp'09. 2nd International Congress, 2012.

[9] Ansari M. D., Ghrera S. P. and Tyagi V., "Pixel-based image forgery detection: A review", IETE journal of education, 55(1), 40-46, 2014.
[10] Mehta V., Jaiswal A. K. and Srivastava R., "Copy-Move Image Forgery Detection Using DCT and ORB Feature Set", in International Conference on Futuristic Trends in Networks and Computing Technologies, Springer, 2019.
[11] Kumar, A., A. Bhavsar, and R. Verma. Syn2Real: Forgery Classification via Unsupervised Domain Adaptation. in Proceedings of the IEEE Winter Conference on Applications of Computer Vision Workshops. 2020.
[12] Yang B., et al., "A copy-move forgery detection method based on CMFD-SIFT", Multimedia Tools and Applications, 77(1), 837-855, 2018.
[13] Abdalla Y., Iqbal M. T. and Shehata M., "Convolutional Neural Network for Copy-Move Forgery Detection", Symmetry, 11(10), 1280, 2019.
[14] Dhivya S., Sangeetha J. and Sudhakar B., "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique", Soft Computing, 1-12, 2020.
[15] Chen H., Yang X. and Lyu Y., "Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm", IEEE Access, 8, 36863-36875, 2020.
[16] Wu Y., Abd-Almageed W. and Natarajan P.. "Buster Net: Detecting copy-move image forgery with source/target localization", in Proceedings of the European Conference on Computer Vision (ECCV), 2018.
[17] Bosse S., et al., "A deep neural network for image quality assessment", in 2016 IEEE International Conference on Image Processing (ICIP), IEEE, 2016.
[18] Sadeghi-Tehran P., et al., "Deepcount: in-field automatic quantification of wheat spikes using simple linear iterative clustering and deep convolutional neural networks", Frontiers in plant science, 10, 1176, 2019.
[19] Kaur H. and Kaur K., "A Brief Survey of Different Techniques for Detecting Copy-Move Forgery", International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 875-882, 2015.
[20] Wani M. A., et al., "Advances in deep learning", 57, Springer, 2020.