International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

An Evaluation of Convolutional Neural Network (CNN) Model for Copy-Move and Splicing Forgery Detection

Thiiban Muniappan[1], Nor Bakiah Abd Warif*[2], Ahsiah Ismail[3], Noor Atikah Mat Abir[4]

Submitted: 11/11/2022 **Revised**: 21/01/2023 **Accepted**: 09/02/2023

Abstract: Image forgeries such as copy-move and splicing are very common due to the availability of the advancement in software editing techniques. However, most of the existing methods for forgery detection consider only one type of image forgery due to the reason that both forgeries have different traits. In this paper, a Convolutional Neural Network (CNN) model which is one of the deep learning approaches is simulated and analyzed to detect any forged image without knowing their types of forgeries. In the model, three phases are involved: Data Preprocessing, Feature Extraction, and Classification. The model learns to extract features from convolutional, pooling, and Rectified Linear unit layer, and classified the image whether it is original or forged using fully connected layer. For the experimental works, three datasets namely MICC-F2000 (2000 images), CASIA 1 (1721 images), and CASIA 2 (12615 images) are tested and compared with existing deep learning-based methods. The results show that the CNN model achieved the highest performance with accuracy of 79% for CASIA 1 and 89% for CASIA 2.

Keywords: *Convolutional Neural Network, Deep Learning, Image Forgery Detection*

1. Introduction

Forgery is the action of tampering with a copy or imitation of a document, signature, banknote, or work of art, whereas, image forgery simply means the manipulation of an image to change a few of the meaningful or useful traits of the image. The process of creating forged images has become easy in this era of technology due to the powerful computers with the advanced photo-editing software such as Adobe Photoshop, Gimp, Photo Editor, and etc. These forged images can be used in various ways, it could be just a simple editing for posting in the social media account or it could be an image forgery for cheating purposes. These image forgeries can cause a lot of damage and losses. For example, if a forged image is used as digital evidence in a court of law, it can lead to a misjudgment of the case. However, identifying the forged images by human's naked eyes is very difficult. Therefore, the detection of these forged image copies has becoming an important research topic.

Based on the literature, there are various types of image forgery techniques. Among the forgery techniques, copy-move, and splicing are the common manipulations. Copy-move will copy and paste regions within the same image [1] while splicing copies regions from an original image and paste them to a different image [2]. However, each type of forgery has a different characteristic, thus, it will be difficult for the forensic examiners to cater all these forgeries. As a result, different algorithms and tools are required to detect different types of image forgery. For example, Scale Invariant Feature Transform (SIFT) [3] only focuses on copy-move forgery detection. In this method, the key-points and their descriptors are identified. Then, matching pairs will be grouped based on the spatial distance and geometric constraints to detect if there are any duplicated regions. Furthermore, in existing splicing detection method [2], Local Binary Pattern (LBP) and wavelet transform is applied in all blocks while Principal Component Analysis (PCA) is computed from all blocks. Then, the output will be used as features to classify an image with splicing forgery using the Support Vector Machine (SVM) classifier.

In the real situation, the images to be detected are usually from many kinds of forgery techniques. Thus,

[1] *Centre for Information Security Research, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia*
[2*] *Centre for Information Security Research, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia*
ORCID ID : 0000-0002-6226-2271
[3] *Kuliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia*
ORCID ID : 0000-0003-3057-3734
[4] *Centre for Information Security Research, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia*
** Corresponding Author Email: norbakiah@uthm.edu.my*

identifying the types of forgery will be a major challenge [4]. Therefore, a Convolutional Neural Network (CNN) model from a deep learning approach is replicated to evaluate the performance on both copy-move and splicing forgeries. The CNN model will use the image as an input and assign importance to various objects in the image to differentiate one from another [5]. To evaluate and compare the performance of the model, three datasets are used namely MICC-F2000 (2000 images), CASIA 1 (1721 images), and CASIA 2 (12615 images). The MICC-F2000 [6] dataset consists of the copy-move forgery images and CASIA 1 [7] dataset consists of the splicing forgery images. Meanwhile, CASIA 2 [7] dataset contained both copy-move and splicing forgeries. The results are compared with existing deep learning-based methods.

This paper consists of five parts: Section 2 discusses the literature review, which covers all terms and definitions related to image forgery detection, deep learning, and other research contributions. Section 3 explains about the methodology and CNN model while Section 4 reviews the experimental results. Finally, section 5 concludes this paper.

2. Related Works

This section starts with defining the available image forgery detection and focusing on two types of passive approach namely copy-move and splicing. Since deep learning approach seems popular recently and able to obtain high performance results, this section also discussed the approach and current implementation especially in detecting image forgery.

2.1. Image Forgery Detection Techniques

Image Forgery detection techniques are mainly created to find inconsistent patterns that are supposed to be in the forged image. There are two approaches to detect forgery in the images. They are Active and Passive approaches. The branches of image forgery detection are shown in Fig. 1.

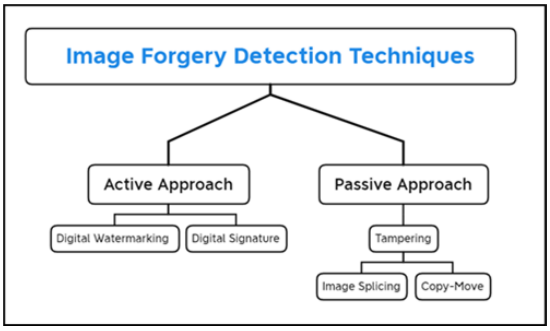


Figure 1. Branches of Image Forgery Detection Techniques.

The active approach needs pre-processed information of the image to be embedded into the image using techniques such as digital signature or digital watermark to detect any forgery in the image. Digital Watermarking and Digital Signature are two main active authentication techniques, as something embedded into the image when they are obtained [8]. The forged image can be detected if the special information cannot be extracted from that obtained image. Digital Signature must be inserted on the image during the recording of the image itself. For Digital Watermarking, a symbol or data should be inserted as watermark on the image during the storing period. The disadvantage of an active approach is it requires human intrusion or specially designed cameras.

In contrast, the passive approach does not require such information about the image to authenticate it. Passive approach also known as the blind approach since it only uses the image itself for its authentication and integrity. The passive methods detect region duplication such as copy-move and splicing. This approach assumes that although the manipulation of image will not leave any visual trace, they are more likely to change the image statistics, and these underlying inconsistencies play a main role in detection of the image forgery.

2.1.1. Copy-Move

Copy-move is a forgery technique that creates a compound picture by copying a region from an image and pasting it to the same image. The challenge in a copy-move is that the copy move region forms is a part of the same picture. It is also harder to classify the manipulated zone in the same image compared to the field of many other image statistical approaches, like image splicing [9].

There are two popular approaches of copy-move forgery detection methods which are block-based and key-point-based. For block-based, Fridrich et al. [10] is the first that initiate the CMF detection by applying Discrete Cosine Transform (DCT) features to find the identical quantization values in their block-matching scheme. This method is used to recognize when a tampered image is saved in lossy format such as JPEG, hence, it is robust to JPEG compression. Then, Popescu et al. [11] proposed a technique that replaces DCT with Principal Component Analysis (PCA) to reduce the feature dimension representation, thus, increase the robustness and sensitivity to additive noise and lossy JPEG compression. In another works, Gani and Qadir [12] combines cellular automata with DCT to be robust to multiple post-processing attacks. Meanwhile, Al-Qershi and Khoo [13] combined features from Zernike Moment to detect CMF with various attacks of rotation and scale.

Another approach, key-point, is for key-point-based CMF detection methods. A set of descriptors is extracted for each point to improve the reliability of the features in CMF detection. Huang et al. [14] proposed the Scale Invariant Feature Transform (SIFT) that detects similarity by an exhaustive search of the SIFT features in an image. Amerini et al. [6] become dominant in CMF detection because the method is better than existing SIFT-based CMF detection, at both scale and rotation attack. Though Mishra et al. [15] replaced the SIFT features with SURF and create the areas from the matching key-point, but the performance is still lower than Amerini et al.'s method. In another study, Uliyan et al. [16] recommended the angular radial partitioning with Harris corner detector to detect CMF duplication in the presence of several geometric transformation. Unfortunately, the method increased the running time of SIFT and SURF features.

2.1.2. Splicing

Splicing is created by copying a region from an image and pasting it onto another image. Therefore, a minimum of two pictures are needed to create a forged image using the image splicing technique. If the pictures that are combined have contrasting foundation, it will be very hard to make the borders and boundaries incoherent [5]. Usually, digital photomontage is created using image splicing to stick two images together via Adobe Photoshop and many other tools.

Various kinds of methods have been proposed to detect image splicing. Some of the methods use traditional block matching, while another method implements machine learning algorithm. For traditional block matching, local binary pattern (LBP) features are used as a feature extractor in two different image splicing detection method [2], [17]. Hakimi et al. [2] combined LBP and Discrete Wavelet Transform (DWT) to extract features from non-overlapping blocks of chrominance part of the image, while Vidyadharan and Thampi [17] focused on multiple texture in detecting splicing image. Meanwhile, by assuming that noise level of splicing region is inconsistent with original image region, Wang et al. [18] proposed Laplacian operator to remove the noise from the image. Then, the regions are grouped together based on related region corrosion to obtain the precise splicing region.

On the other hand, for machine learning classification, Zhao et al. [19] developed image splicing detection method based on 2-D Noncausal Markov Model and classify the image using SVM to determine whether the image has been spliced or not. Then, Wang et al. [20] put forward a method using Markov of quaternion component separation in the quaternion discrete cosine transform (QDCT) domain and quaternion wavelet transform (QWT) domain. To improve the accuracy of this process, an ensemble classifier is used to differentiate authentic and spliced color images.

Recently, Kanwal et al. [21] employs an optimal threshold value to improve the enhanced local ternary pattern (ELTP) texture descriptor in overlapping block and identify the image forgery using SVM. In contrast, Jaiswal and Srivastava [22] proposed a hybrid method by combining four features: HoG, LTE, DWT, and LBP while a logistic regression classifier is employed to determine the image's authenticity.

2.2. Deep Leaning Approach

Deep Learning is a subset of machine learning that teaches computers to do things that humans do naturally. The key difference between the basic machine learning and deep learning is that machine learning manually driven features from the sample data, while deep learning specializes on learning the features of the sample data or the representations from the sample data automatically without human intrusion. Deep learning has multiple invisible layers and raw data can be trained and learn directly from the input driven features and representations [23]. Deep learning is also a well-known technique that is able to extract high level features to learn from the raw input directly. Recently, the growth of deep learning has rapidly increased with convincing results. Thus, forensic researchers are using deep learning approach to detect manipulations of images without human intrusion [9].

2.2.1. Image Forgery Detection using Deep Learning

Work by Zhang et al. [25] recommended a two-step deep learning approach for detecting forged images that might be in various formats. In the first step, the images are converted into YCrCb color space and segmented into 32 x 32 patches. Then, a 3 Level 2D Daubechies Wavelet decomposition is applied to each YCrCb component of patches. Standard deviation, mean and sum for each of the approximation, horizontal, vertical, and diagonal coefficients are calculated to obtain the features. After that, the images are separated into areas and used the Loaded Auto-encoder model to find out the structures for every spot.

They compare the results of JPEG and TIFF images in both types of forgery.

Meanwhile, Salloum et al. [26] suggested a deep learning approach to detect image splicing forgery by using a Multi-Task Fully Connected Network. Multi-Task Fully Connected Network works better than Single-Task Fully Connected Network because the network delivers irregular and inconsistent output for localization in some cases. The Multi-Task Fully Convolutional Network is designed with a set of output branches. One branch is used to learn the surface label and the other branch is used to learn the boundary of the spliced region. The branches are used to acquire surface label information and the edges of interfered sections. The probability maps lead to a finer localization of the spliced region.

In contrast, work by Koul et al. [1] suggested a deep learning approach to detect copy-move forgery by using a CNN. In CNN, the image datasets are divided into training and testing sets. Then, the features that are extracted from the image are sent to the CNN model for the classification process. The features of the images will be automatically identified and passed down to the deep learning classifier model for classification. Similarly, to detect a copy-move forgery, Goel et al. [27] proposed a dual branch of CNN that implements different kernel sizes for feature extraction. However, both works are not tested on the splicing images, hence, the efficiency on the types of images is absent.

Recently, Mallick et al. [28] compared three different CNN models with Error Level Analysis, VGG16 and VGG 19 to detect both copy-move and splicing forgery detection. On the other hand, Qazi et al. [29] proposed a CNN by using the architecture of ResNet50v2 and utilizes weight of YOLO CNN also for both, copy-move and splicing forgery detection. The results are presented in the Section 4.3.

3. Methodology

This section describes the deep learning approach for image forgery detection using a CNN model. The model is illustrated in Fig. 2 which consists of three main phases specifically image preprocessing, feature extraction and classification. The feature extraction is done in layers such as the Convolution layer, Pooling layer, and Rectified Linear Units (ReLU) layer while the classification is done in the Fully Connected layer.

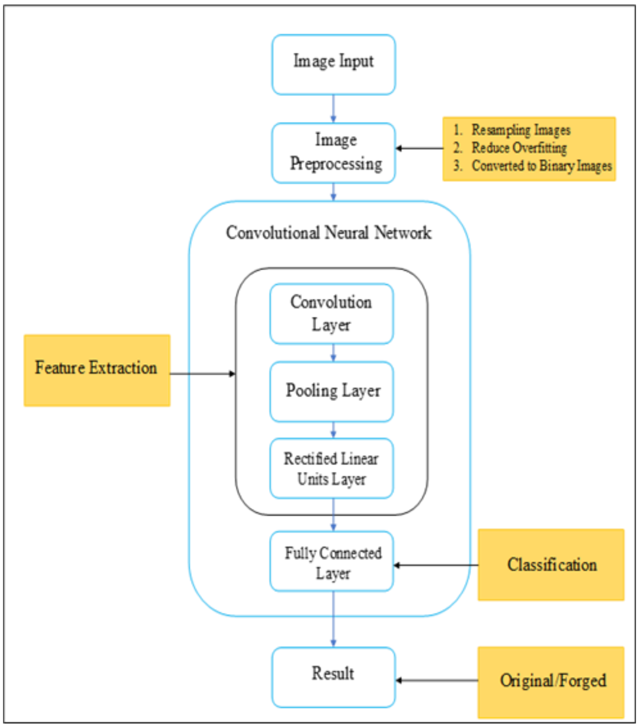


Figure 2. The Framework of Analysis on Image Forgery Detection Using Convolutional Neural Network.

3.1. Image Pre-processing

Image pre-processing is an important phase in forgery detection for both copy-move and splicing forgery. Before testing the model, images from the datasets must be pre-processed to improve them. This is because the images from the datasets might contain noise, blurriness, poor lighting conditions, and low-quality camera.

In this phase, the images from the datasets will be resized to the target size. The size is 128 x 128, and the image will be converted into an Error Level Analysis image. By reducing the size of these images, the training time can be improved drastically without significantly reducing the model's performance. Then, the Image Data Generator class from Tensor Flow library will be used to perform these pre-processing steps.

3.2. CNN Model

After the input image is pre-processed, it will be subjected to CNN model. The CNN model consists of convolution layers, pooling layers, Rectified Linear Units (ReLU) layers and fully connected layers which are also known as dense layers. In this model, convolution layers, pooling layers, Rectified Linear Units (ReLU) layers will perform feature extraction, while the next layer which is the fully connected layer will map the extracted features into final output, which is known as classification. The common CNN architecture may have a repetition of several convolution layers, a pooling layer and one or more fully connected layers [5]. Fig. 3 shows the CNN model that is used for both feature extraction and classification.

hyperparameters which are the size and the number of kernels. The former is typically 3 x 3 but for this study, 7 x 7 is also used. Stride is known as the distance between two consecutive kernel locations, and it is commonly used preference in the CNN model [5]. In this model, the stride used is 3 to achieve down sampling of the feature maps.

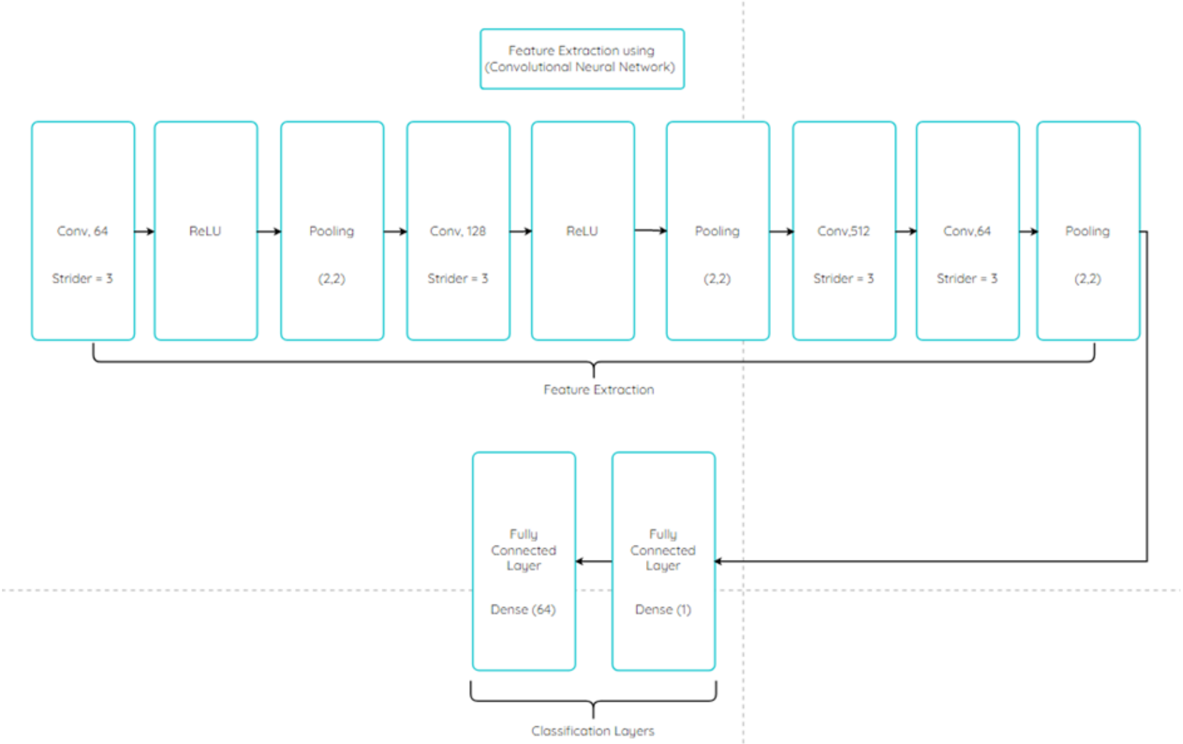


Figure 3. Convolutional Neural Network Model.

3.2.1. Feature Extraction

During feature extraction, features from deeper layers will be conveyed to higher levels. These features are built from the lower levels by integrating the features that are found in the early layers. Therefore, a feature extractor is included in the training phase of CNN, which consists of convolution layers followed by an activation function, pooling layers, and fully connected layers.

- **Convolution Layer**

A convolution layer is an important part of the CNN model. This layer is a specialized type of linear operation that performs feature extraction. A small array of numbers called kernel, is applied across the input from the dataset which is in an array of numbers called input tensor. When the value of the dot product between each element of the kernel and the input tensor is obtained, a feature map is produced. The convolution operation is defined with two key

- **Pooling Layer**

In the pooling layer, a down-sampling operation will be performed. This operation is performed to reduce the number of learnable parameters and the dimensionality of feature maps produced in the convolution layer [5]. There are two commonly used forms of pooling which are max-pooling and average pooling [23]. Max pooling extracts patches from the feature maps and gives an output of the maximum value in each patch and discards the other values. For this model, max pooling with a filter size of 2 x 2 is used to down sample the in-plane dimension of the feature maps by a factor of 2. However, the depth dimension of the feature maps remains unchanged.

- **Rectified Linear Units Layer**

The outputs of the linear operation layers which are the convolution and pooling layers are then passed through a non-linear activation function [5]. There are many nonlinear graph functions such as sigmoid, hyperbolic, and rectified linear unit (ReLU) that can be used as the activation function. In this research, ReLU is chosen as the nonlinear activation function because it can train the model faster without making any significant changes to accuracy [24]. This function changes the output to the value of f(x) = max(0,x). Fig. 4 shows the graph function of the rectified linear unit (ReLU).

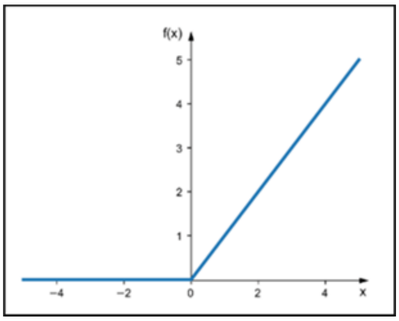


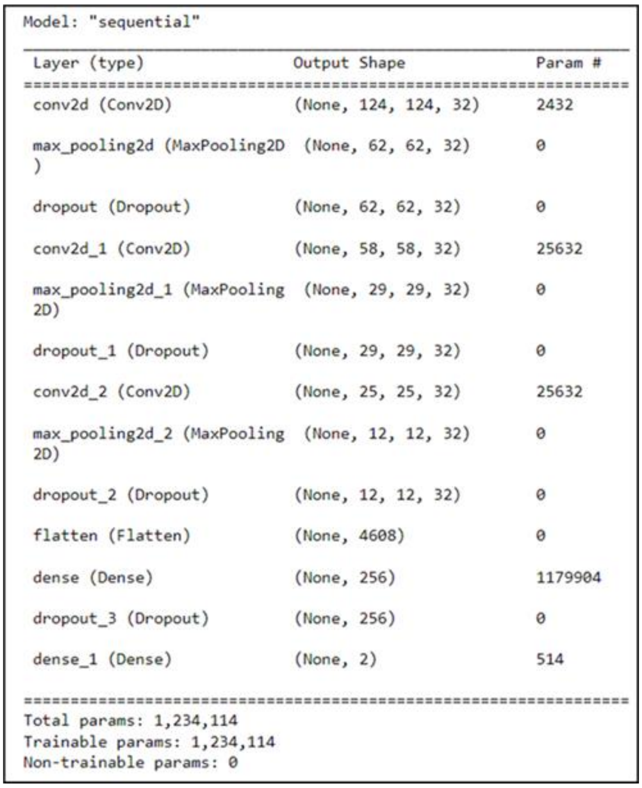
Figure 4. Graph Function of Rectified Linear Unit (ReLU).

3.2.2. Image Classification

Deep Learning is a machine learning method where the model can learn itself to perform image classification automatically. Deep Learning has the upper hand due to the presence of multiple filters in the training phase. As part of a deep learning model, the final layer is the fully connected layer mapped to a dense layer. The dense layer will convert the output of the fully connected layer into a probability of each image or object being in a certain class.

- **Fully Connected Layer**

The fully connected layer is used in the classification process. The feature maps of the last convolution or the pooling layer will usually be converted into a one-dimensional array of numbers. Then, this array will be connected to one or more fully connected layers. This layer is also known as the dense layer. In the dense layer, every input is connected to every output by a learnable weight [5]. Once the extracted features from the convolution layers are down sampled by the pooling layers, they are mapped by a subset of a dense layer to the final output of the Convolutional Neural Network (CNN). In this research, two fully connected layers will be used to get a better prediction. Fig. 5 shows the summary of the CNN model that is used in this paper. The model consists of repetition of three convolution layers, three pooling layers and two fully connected layers.



```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 124, 124, 32)      2432

 max_pooling2d (MaxPooling2D  (None, 62, 62, 32)       0
 )

 dropout (Dropout)           (None, 62, 62, 32)        0

 conv2d_1 (Conv2D)           (None, 58, 58, 32)        25632

 max_pooling2d_1 (MaxPooling  (None, 29, 29, 32)       0
 2D)

 dropout_1 (Dropout)         (None, 29, 29, 32)        0

 conv2d_2 (Conv2D)           (None, 25, 25, 32)        25632

 max_pooling2d_2 (MaxPooling  (None, 12, 12, 32)       0
 2D)

 dropout_2 (Dropout)         (None, 12, 12, 32)        0

 flatten (Flatten)           (None, 4608)              0

 dense (Dense)               (None, 256)               1179904

 dropout_3 (Dropout)         (None, 256)               0

 dense_1 (Dense)             (None, 2)                 514

=================================================================
Total params: 1,234,114
Trainable params: 1,234,114
Non-trainable params: 0
```

Figure 5. CNN model used for Feature Extraction and Image Classification.

4. Experimental Results and Discussion

This section discusses the details of the experimentation of image forgery detection using CNN model including the performances. Firstly, the datasets used in the experiments are described. Then, the results between two types of forgeries are compared based on accuracy, precision, recall and F1-score performance. Since there are limited research work on deep learning approach specifically on both, copy-move and splicing forgery detection, we also include other related studies that suit the focus of this research in the last sub section.

4.1. Dataset as the input image

There are three datasets implemented as inputs for these experiments. One dataset represents copy-move forgery, namely MICC-F2000 dataset from the Media Integration and Communication Center of Universita Degli Study di Firenze [6]. This dataset consists of 700 images with copy-move forgery and 1300 original images. The other datasets are CASIA 1 and CASIA 2 from the Chinese Academy of Sciences, Institute of Automation [7]. CASIA 1 dataset consists of 921 images with splicing forgery and 800 original images. Meanwhile, CASIA 2 dataset combines both forgery techniques in 5123 forged images with 7492 original images. Since only CASIA 2 dataset provides two forgeries in a dataset, we combined the MICC-F2000 with CASIA 1 for additional experiments. For the experimental works, all datasets are split for training and testing with the ratio 60:40. 60% of the datasets are used for training and 40% of it is used for testing. All datasets are trained for 30 times (30 epochs) with 64 batch size using the CNN model.

4.2. Parameter Evaluation

For evaluation, the forged images are considered as positive class while the original images are considered as negative class. The equations can be defined as:

- Positive (P): The image is forged.
- Negative (N): The image is original.
- True Positive (TP): The image is forged, and it is predicted to be forged.
- False Positive (FP): The image is original, and it is predicted to be forged.
- False Negative (FN): The image is forged, and it is predicted to be original.
- True Negative (TN): The image is original, and it is predicted to be original.

In this research, the performance is measured in terms of accuracy as computed in Eq. (1). Other measures such as precision, recall and F1-score, are also being analyzed. Accuracy is the percentage of samples being accurately predicted as forged or original to the total number of the images tested.

$$Accuracy = ((TP+TN))/(TP+TN+FP+FN) \quad (1)$$

Table 1. The Experimental Results – Accuracy for all datasets.

Parameter/Dataset	MICC-F2000 Dataset (Copy-move Forgery)	CASIA 1 Dataset (Splicing Forgery)	CASIA 2 Dataset (Both Forgeries)	MICC-F2000 +CASIA 1
Accuracy	0.76	0.79	0.89	0.7

Precision is the ability of a classifier to detect the forgery that is in fact a forgery. It is the proportion of correct positive predictions and is given by the formula as shown in Eq. (2). Recall is a unit which measures the ability of a classifier to find all the ground-truths. Recall also represents the probability of the forged image being detected. It is the proportion of true positive detected among all ground-truths and is given by the formula as shown in Eq. (3). F1-score is a harmonic mean of precision and recall. This is used to combine both precision and recall in a single value with the formula as shown in Eq. (4).

$$Precision = TP/(TP+FP) \quad (2)$$

$$Recall = TP/(TP+FN) \quad (3)$$

$$F1-Score = 2\,((Precision \times Recall)/(Precision+Recall)) \quad (4)$$

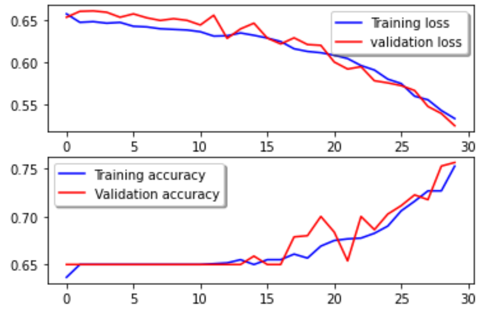
4.3. Results and Analysis

Table 1 shows the result of accuracy for all the datasets which are MICC-F2000 for copy-move forgery, CASIA 1 for splicing forgery, CASIA 2 and MICC-F2000+CASIA 1 for both forgeries. Based on the table, the results show that the CNN model able to differentiate splicing forgery (79%) more accurately than copy-move forgery (76%). Considering that accuracy calculates all the images in the dataset, CASIA 2 shows the highest performance with 89% accuracy. This is due to the reason that the dataset consists both of forgeries and contains many images to be trained. In contrast, the performance decreased when tested with the combination of MICC-F2000+CASIA 1 with 70% accuracy. This is because the number of copy-move image is 200 less than splicing image. While in CASIA 2, the total copy-move image is much smaller than splicing image. It is proved that the CNN model works well with splicing compared to copy-move forgery. Moreover, the model has several difficulties to differentiate various types of forgery in one classification as shown in graph listed in table 2. As can be seen from the presented graph in Table 2, the loss and accuracy are maintained if only one type of forgery is evaluated. Contrarily, the stability of graph is affected when both forgeries are combined in one dataset. Besides, the number of losses also become higher when the copy-move images are involved in the dataset.

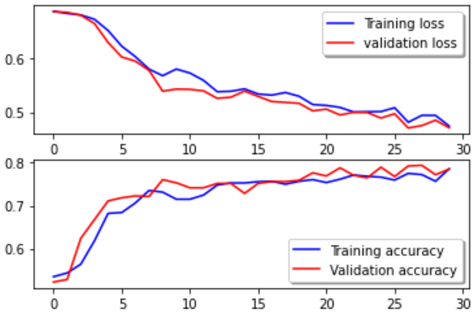
Difference with accuracy, precision calculates the number of correctly images detected including the wrongly detected images while recall computes only the number of correctly detected images over the class. Therefore, since F1-score considers both precision and recall, the score is significant to be further measured and examined. Table 3 lists all the results of performance measures of precision, recall and F1-score for all classes in the dataset. As we can see from the table, the CNN model only able to detect 57% score of all copy-move images in the MICC-F2000 with 83% of score for original images. Meanwhile, the results for CASIA 1 show that the model able to detect 82% score of splicing images and 74% score of original images. Since the results are based on the training images, the model tends to misclassify copy-move forgery images as original images in MICC-F2000 dataset and original images as splicing forgery images in CASIA 1 dataset.

Table 2. Training and Validation Loss and Accuracy Graph of the Three Datasets.

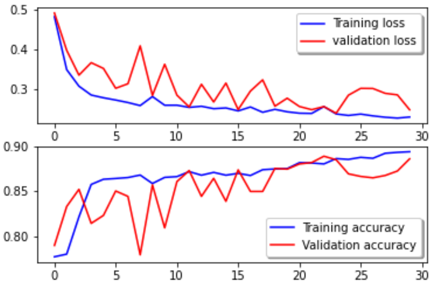
Training and Validation Loss and Accuracy Graph



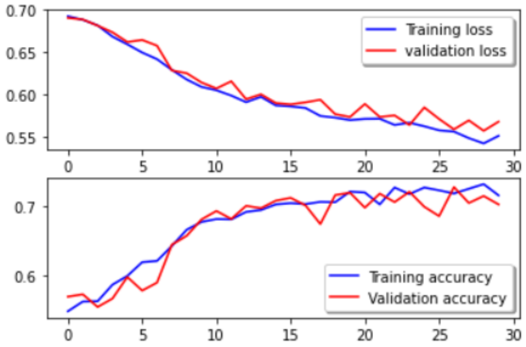
MICC-F2000



CASIA 1



CASIA 2



MICC-F2000+CASIA 1

Table 3. The Experimental Results – specific class.

Dataset	Class	Precision	Recall	F1-Score
MICC-F2000	Forged	0.75	0.45	0.57
	Original	0.76	0.92	0.83
CASIA 1	Forged	0.74	0.91	0.82
	Original	0.87	0.65	0.74
CASIA 2	Forged	0.67	0.90	0.77
	Original	0.97	0.88	0.92
MICC-F2000+CASIA 1	Forged	0.69	0.56	0.62
	Original	0.71	0.81	0.97

On the other hand, the score for CASIA 2 dataset shows that the model achieved 77% score for forged images and 92% score of original images. Similar nature can be seen for the score of the combination of MICC-F2000 with CASIA 1 when the score for forged images detection is 62%, which is lower than original images detection which is 97%. This might be because both datasets contain copy-move forgery images, thus, resulting almost similar results with MICC-F2000 dataset. The model tends to misclassify copy-move forgery images as original images. Fig. 6 shows an example of misclassify an original image as copy-move image due to the repetition of various regions in the images.

Figure 6. Example of misclassify an original image as forged image.

To further evaluate the performance of the CNN model, the results are compared with existing deep learning-based methods. Table 4 shows the comparison results with Goel et al. [25] and Koul et al.'s method [1] using MICC-F2000. Even though the result shows that their method achieved higher performance compared to the CNN model, their method does not include image splicing detection. Different with the results in Table 5, the CNN model is able to be more precise than Zhang et al.'s method [23] with 81% for combine CASIA, more accurate than Qazi et al.'s method [26] with 79% for CASIA 1 and 89% for CASIA 2 and achieve higher F-score than Salloum et al.'s method [24] with 82%. This is because the CNN model is able to work well with splicing and the combination of splicing and copy-move forgery detection.

5. Conclusion

Image Forgery is a challenging threat in the digital forensic world due to various types of image forgery. Thus, an efficient forgery detection technique is needed to counter this problem. Due to different behaviors encountered in both copy-move and splicing forgery, there are limited studies on image forgery detection that consider both types of forgery. Therefore, this research simulated a CNN model on three different datasets. The accuracy performance of the CNN model is evaluated for three different datasets which consist of copy-move forgery, splicing forgery and both forgeries. The reason of using dataset that consists of the combination for both forgeries is because in real situations environment, the types of forgeries present in the image is unknown; it could be copy-move or splicing. The experimental test results show the CASIA 2 dataset which consists of both forgeries with a high-volume image achieved the highest accuracy with 89%, while CASIA 1 dataset that represents splicing forgery obtained 79%. Furthermore, the result shows that the CNN model works well with the splicing forgery compared to copy-move forgery with the accuracy attained only 76% on the MICC-F2000 dataset. Based on these results, we believed that the CNN model is able to effectively detect both forgeries especially in a large dataset which consist of a balance number of trained image forgery.

Table 4. Comparison Results – MICC-F2000 dataset.

Dataset	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Goel et al. **[25]**	0.96	0.89	1	0.94
Koul et al. **[1]**	0.98	0.97	0.96	0.97
CNN model	0.76	0.76	0.69	0.7

Acknowledgements

This research was supported by Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2020/ICT04/UTHM/02/1).

Table 5. Comparison Results – CASIA dataset.

Dataset/ Method	**Combine CASIA (JPEG)**			**CASIA 1**		**CASIA 2**
	Accuracy	**Precision**	**Recall**	**Accuracy**	**F1-Score**	**Accuracy**
Zhang et al. **[23]**	0.87	0.60	0.93	-	-	-
Salloum et al. **[24]**	-	-	-	-	0.54	-
Mallick et al. **[27]**	-	-	-	-	-	0.73 (combine with NC2016)
Qazi et al. **[26]** without transfer learning	-	-	-	0.69	-	0.80
CNN model	0.85	**0.81**	0.83	**0.79**	**0.82**	**0.89**

Author contributions

Thiiban Muniappan[1]: Writing-Original draft preparation, Methodology, Software, Field study
Nor Bakiah Abd Warif[2]: Data curation, Writing-Reviewing and Editing, Validation, Field study
Ahsiah Ismail[3]: Visualization, Investigation, Writing-Reviewing and Editing
Noor Atikah Mat Abir[4]: Writing-Second draft, Field study

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] S. Koul, M. Kumar, S. S. Khurana, F. Mushtaq and K. Kumar, "An efficient approach for copy-move image forgery detection using convolution neural network," *Multimedia Tools and Applications,* vol. 81, no. 8, p. 11259–11277, 2022.

[2] F. Hakimi, M. Hariri and F. GharehBaghi, "Image splicing forgery detection using local binary pattern and discrete wavelet transform," in *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI),* Tehran, Iran, 2015.

[3] X. Y. Wang, L. X. Jiao, X. B. Wang, H. Y. Yang and P. P. Niu, ".A new keypoint-based copy-move forgery detection for color image," *Applied Intelligence,* vol. 48, no. 10, p. 3630–3652, 2018.

[4] B. S. Kumar, S. Karthi, K. Karthika and R. Cristin, "A systematic study of image forgery detection," *Journal of Computational and Theoretical Nanoscience,* vol. 15, no. 8, pp. 2560-2564, 2018.

[5] R. Yamashita, M. Nishio, R. K. G. Do and K. Togashi , "Convolutional neural networks: an overview and application in radiology," *Insights into Imaging,* vol. 9, no. 4, pp. 611-629, 2018.

[6] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security,* vol. 6, no. 3, pp. 1099-1110, 2011.

[7] J. Dong, W. Wang and T. Tieniu, "CASIA Image Tampering Detection Evaluation Database," in *2013 IEEE China Summit and International Conference on Signal and Information Processing,* 2013.

[8] V. Sharma, S. Jha and R. K. Bharti, "Image Forgery and it's Detection Technique: A Review," *International Research Journal of Engineering and Technology (IRJET),* vol. 3, no. 3, pp. 756-762, 2016.

[9] M. H. Alkawaz, G. Sulong, T. Saba and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Computing and Applications,* vol. 30, no. 1, p. 183–192, 2018.

[10] J. Fridrich, D. Soukal and J. Lukas, "Detection of copy-move forgery in digital images," *International Journal Computer Science,* pp. 652-663, 2003.

[11] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," 2004.

[12] G. Gani and F. Qadir, "robust copy-move forgery detection technique based on discrete cosine transform and cellular automata," *Journal of Information Security and Applications,* vol. 54, p. 102510–102524, 2020.

[13] O. M. Al-Qershi and B. E. Khoo, "Enhanced block-based copy-move forgery detection using k-means clustering.," *Multidimensional Systems and Signal Processing,* vol. 30, no. 4, p. 1671–1695, 2019.

[14] H. Huang, W. Guo and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, 2008.

[15] P. Mishra , N. Mishra, S. Sharma and R. Patel, "Region Duplication Forgery Detection Technique Based on SURF and HAC," *The Scientific World Journal,* p. 1–8, 2013.

[16] D. Uliyan, H. Jalab, A. W. A. Wahab and S. Sadeghi, "Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points," *Symmetry,* vol. 8, no. 7, p. 62, 2016.

[17] D. S. Vidyadharan and S. M. Thampi, "Digital image forgery detection using compact multi-texture representation," *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 4, p. 3177–3188, 2017.

[18] X. Wang, Q. Zhang, C. Jiang and Y. Zhang, "Coarse-to-fine Grained Image Splicing

Localization Method Based on Noise Level Inconsistency," in *2020 International Conference on Computing, Networking and Communications (ICNC)*, 2020.

[19] S. W. Zhao, L. Shenghong and L. Jianhua, "Passive Image-Splicing Detection by a 2-D Noncausal Markov Model," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 2, p. 185–199, 2015.

[20] R. Wang, W. Lu, J. Li, S. Xiang, X. Zhao and J. Wang, "Digital Image Splicing Detection Based on Markov Features in QDCT and QWT Domain," *International Journal of Digital Crime and Forensics*, vol. 10, no. 4, p. 90–107, 2018.

[21] N. Kanwal, A. Girdhar, L. Kaur and J. S. Bhullar, "Digital image splicing detection technique using optimal threshold based local ternary pattern," *Multimedia Tools and Applications*, vol. 79, no. (19-20), p. 12829–12846, 2020.

[22] A. K. Jaiswal and R. Srivastava, "A technique for image splicing detection using hybrid feature set.," *Multimedia Tools and Applications*, vol. 79, no. (17-18), p. 11837–11860, 2020.

[23] A. Kaur, Y. Singh, N. Neeru, L. Kaur and A. Singh, "A Survey on Deep Learning Approaches to Medical Images and a Systematic Look up into Real-Time Object Detection," *Archives of Computational Methods in Engineering* , pp. 2071-2111, 2022.

[24] Y. Zhang, G. Jonathan, L. W. Lei and T. Vrizlynn, "Image Region Forgery Detection: A Deep Learning Approach," in *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016*, 2016.

[25] R. Salloum, Y. Ren and C. -C. J. Kuo, "Image Splicing Localization using a Multi-task Fully Convolutional Network (MFCN)," *Journal of Visual Communication and Image Representation*, vol. 51, pp. 201-209, 2018.

[26] N. Goel, S. Kaur and R. Bala, "Dual branch convolutional neural network for copy move forgery," *IET Image Processing*, vol. 15, pp. 656-665, 2021.

[27] D. Mallick, M. Shaikh, A. Gulhane and T. Maktum, "Copy Move and Splicing Image Forgery Detection using CNN," in *International Conference on Automation, Computing and Communication 2022 (ICACC-2022)*, 2022.

[28] E. U. H. Qazi, T. Zia and A. Almorjan, "Deep Learning-Based Digital Image Forgery Detection System," *Applied Science*, vol. 12, no. 2851, pp. 1-17, 2022.