A New Deep Learning Based Technique To Detect Copy Move Forgery In Digital Images

Akhila M P[1], Aiswariya Raj [2] , Manju C P[3]

[1] *Electronics and Communication Engineering Federal Institute of Science And Technology Kerala, India*
[2]*Assistant Professor Electronics and Communication Engineering Federal Institute of Science And Technology Kerala, India*
[3]*Assistant Professor Electronics and Communication Engineering Federal Institute of Science And Technology Kerala, India*

---***---

Abstract - *Due to the advancement of photo editing software, digital image forgery detection has become an active research area in recent years. In recent studies, deep learning-based methods outperformed hand-crafted methods in image tasks such as image classification and retrieval. As a result, the proposed method introduces a novel deep learning-based forgery detection scheme. The feature vectors are extracted using the VGG16 CNN model. After obtaining the features, the similarity between the feature vectors was investigated for the detection and localization of forgery. The test result is then compared with two other methods, and the corresponding F1-measures are computed.*

Key Words: **Copy Move Forgery, Deep Learning, VGG16,CNN architecture, block based forgery detection**

1.INTRODUCTION

In today's technology environment, the Digital images are becoming a concrete information source as imaging technology progresses. They are usually seen in defence work, reporting work, medical checkups, and media work. With developments in digital image technology, such as camera equipment, programmes, and computer systems, as well as increased use of internet media, a digital image can now be considered a crucial knowledge point. Because of technical advancements and the availability of low-cost hardware and software modification equipment, as well as enhanced altering tools, picture alteration is now easier and requires less effort. Meanwhile, a wide range of picture manipulation software has put image authenticity in jeopardy. The goal of image content forgeries is to make modifications in such a way that they are difficult to detect with the naked eye, and then utilise the results for harmful purposes. So the, Photographs that have been forged are becoming more common. Without a question, image authenticity is a major worry these days. To validate the legitimacy of the modified image, there are two basic forms of image forgery detection. The first is the active technique, while the second is the passive technique.

Digital watermarking and digital signature are two active methods. Whereas the passive approaches include image splicing, retouching, and copy move forgery. Among different types of forgery, the copy-move method has developed so much that it has become very difficult to find it out at a glance. The method of copy move forgery is to copy a part of the image and cunningly paste it to another part of the same image. Since the copied part of the image is pasted to the same image, so most of the image properties will be same that makes detection difficult. And the Copy move forgery detection which is a passive detection approach can be carried out without the use of PhotoShop or any other software.

Generally, three methods are commonly employed to detect forgery: methods that are block-based, keypoint-based, or a combination of both. The block-based techniques divide the images into overlapping regular blocks and find the fit between each and every block of the entire image. Block-based techniques are more accurate but the segmentation of the image into overlapping blocks makes the approach computationally expensive. Keypoint based techniques perceive the keypoints of an image and use it to discover the copy-pasted forged region. All the above methods mentioned uses hand-crafted features. And the disadvantages of this method is that , these methods have high execution time and at low contrast these methods cannot detect forgeries. And to cope up with this problems, a new deep learning based technique to detect copy move forgery is presented .

The paper is organized as in the following manner. The related works are discussed in Section 2. Section 3 discribes the proposed method. The results of proposed method is discussed in Section 4. And the paper is concluded in Section 5.

2. RELATED WORKS

Different image copy-move forgery detection techniques are considered and analyzed for the period range between (2003-2021) in this section. A recent study of copy move forgery detection mainly focus on using the SIFT algorithm. Also, most algorithms detect the copy-move forgery when the copy region did not scale and rotate. And most of the copy move forgery detection algorithms is having a very complex procedure for detecting forgery. J Fridrich et.al presented a paper [1] in 2003. This paper investigates the problem of detecting the copy move forgery and describe an efficient and reliable detection method. Also, introduced two algorithms for the detection of copy-move forgery-one that uses an exact match and one that is based on an approximate match. Popescu et.al presented a paper [2] in 2004.This paper describes an efficient technique that automatically detects duplicated regions in digital images. Basically the technique works by first applying a principle component analysis to small fixed size image blocks to yield a reduced dimension representation. And due to some additive noise or lossy compressions the image is robust to minor variations. Although it shows that the detection is possible even in the presence of significant amounts of corrupting noise.

K Sunil et.al presented [3] in 2014. In this paper block matching algorithm is used to detect the type of tampering in this method. Different sized images are taken to evaluate the performance of the proposed algorithm. This algorithm is implemented in matlab 2012a. And the major challenges of this method was not the Robustness against post processing operations and the time taken by the detection technique. Discrete cosine transform and principal component analysis have been used to represent and compress the feature vector of overlapping blocks respectively. This method, on the other hand, successfully detected the copied moved part with intensity changes. N Huang et.al presented [4] in 2018. The proposed method introduced image tampering detection based on CNN and understands extracted features from each convolutional layer and detect different types of image tampering through automatic feature learning. The method involves construction of an image forgery detecting network, that has a total number of nine layers including the input layer, 5 convolutional layer, 2 fully connected layer and a softmax classifier. This method utilized a public dataset, CASIA V1.0 for the experiment analysis. The dataset contains two types of images, authentic and spliced images both in JPEG format. Finally the performance of the proposed method is compared between softmax and SVM in order to demonstrate the advantage. And it was implemented in Matlab 2018b. N H Rajini proposed Image forgery detection using CNN [5] in 2019. This paper presented a novel image forgery identification method which dealt with splicing and copy move forgeries. That is, a technique for detecting image forgery is introduced that combines ZM -polar (Zermike moment) and block discrete cosine transform (BDCT). S S Narayanan et.al introduced [6] in 2020.The proposed method utilizes the advantages of both key point based and block based forgery detection methods. In such an algorithm, the image is segmented into non-overlapping blocks, and for each blocks the key points are computed. And based on a predefined similarity threshold the forged region is identified in this method.

K Sunitha et.al presented copy move forgery detection method using hybrid feature extraction [7] in 2020. This paper also uses both key-point and block-based method for detecting the copy move forgery. And this method does not extract enough feature points considering small and smoothed region. However, this paper presents an effective technique using key-points employing hybrid feature extraction, detection and hierarchical clustering method. And finally the experimental results shows that this method attains better performance when compared with other forgery detection methods. R Agarwal et.al presented [8] in 2020. It was based on the classification of various types of image forgery techniques. Also discusses basic CNN architecture which is used by most deep learning approaches. This paper also presents a comparative analysis of various deep learning methods ,their effectiveness and limitations. I T Ahmed et.al proposed image splicing detection [9] in 2021. The proposed method introduced a CNN based pretrained Alexnet model to extract deep features with little training time. CCA was utilized for the classification purpose. Deep Learning reduces the amount of time and effort required to extract hand-crafted characteristics from manipulated images. Z N Khudhair et.al presented review on copy move forgery detection [10] in 2021. This paper mainly focused on copy move forgery detection and most of the recent algorithms are analyzed and the performances are also compared.

3. PROPOSED METHOD

The proposed method introduces a new deep learning-based detection scheme to detect the forgery. Firstly, the overlapped square blocks are obtained from the input image with the size of 64. After that the CNN architecture is implemented. Here, in the proposed model we have introduced the VGG16 model to extract the feature vectors. After obtaining the feature vectors, similarity matching is done using the Euclidean distance measure. Then the distances are compared with a predetermined threshold value. For this the shift vector between the matched blocks are calculated. Finally, the copy move forged region is detected. In general, proposed method can be explained in three steps:

- Deep learning-based feature extraction
- Feature matching
- Post -processing

3.1 DEEP LEARNING BASED FEATURE EXTRACTION

Initially, the image with a size of 64 is used to obtain the overlapped sub-square blocks. The CNN architecture is then used to extract block features. Here, we've gone with the VGG16 model. VGG16 is a convolution neural net (CNN) architecture that won the 2014 ILSVR (Imagenet) competition. It is widely regarded as one of the best vision model architectures. The 16 in VGG16 refers to the fact that it has 16 layers with weights. This network is fairly large, with approximately 138 million parameters. We use the feature from the maxpool layer of the VGG16 model's block 5 "conv3" layer. Each block is represented by 512-dimensional feature vectors. Then the PCA method is used to reduce dimension.

3.2 FEATURE MATCHING

In this step, the similarity searching is performed after obtaining feature matrix in order to reveal the presence of forgery. To accomplish this, feature matrix is first lexicographically sorted to speed up the matching step. The similarity of vectors is then presented using Euclidean distance. Eq. (1) compares vector distances to a predetermined threshold to determine the matching vectors.

$$f^i = (f_1^i, f_2^i, \dots f_{10}^i), \sqrt{\sum_{k=1}^{10} (f_k^i - f_k^j)^2} \le \partial \qquad (1)$$

To avoid false matches, the candidate matches are checked according to the Euclidean distance among the matched blocks. And it must be greater than the threshold represented. When (x_i, y_i) is the upper left coordinate of $f^i$and (x_j, y_j) is the upper left coordinate of f^j, the distance 'd' is calculated as:

$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \qquad (2)$$

And the condition of $d \ge \beta$ must be provided for the matching of two vectors.

3.3 POST-PROCESSING

In this step, potential false matches are first eliminated. The shift vector between matched blocks is computed for this purpose. (x_i, y_i) and (x_j, y_j) are the upper left coordinates of the suspicious pairs, and the shift vectors are obtained using, $|x_i - x_j|$, $|y_i - y_j|$ values. And it is determined whether the number of blocks with the same shift vector exceeds a predetermined threshold value. If this condition is met, it is proven that copy move forgery has occurred with the related block.

4. RESULTS AND DISCUSSION

In order to further illustrate the efficiency of the proposed method, its results are compared to, two other CNN models. For comparison, the CNN models ResNet50 and Efficient net were utilized. It is also mentioned that the proposed method, as well as others, was tested on the CoMoFoD v2.0 image dataset [11].

4.1 DATASET

Here the test images are taken from the CoMoFoD dataset, that consist of 260 tampered examples. For every tampered image, we stored original image, two types of masks that mark forgery, and additional information such as size of tampered region. These color images range in resolution from 512 × 512 pixels. Some of images from the CoMoFoD v2.0 image dataset are shown in Fig.1.

Fig-1: CoMoFoD v2.0 image dataset samples. The first row has original images, while the second row contains Forged images.

4.2 EVALUATION METRICS

For the performance evaluation of the proposed model ,the F1-measure is calculated based on the confusion matrix. The F1-measure is used for performance evaluation of the considered and proposed methods. Higher F1-measure result indicates its superior performance to marking the forged regions.

$$\text{Precision (p)} = \frac{\text{Tp}}{\text{Tp} + \text{F}_\text{p}}$$

$$\text{Recall(r)} = \frac{\text{T}_\text{p}}{\text{T}_\text{p} + \text{F}_\text{N}}$$

$$\text{F1-Measure} = 2 * \frac{Tp}{2*Tp + F_N + Fp}$$

Where T_p denotes the number of truly detected tampered blocks, F_p denotes the number of incorrectly detected tampered blocks, and F_N denotes the number of incorrectly non-detected blocks.

4.3 PERFORMANCE EVALUATION OF PROPOSED METHOD

In the performance evaluation, the test results of our proposed method is compared with two other CNN models, ie, ResNeT50 and EfficientNet model. ResNet is an acronym for Residual Network. ResNet has many variants that use the same concept but have different numbers of layers. Resnet50 is a variant that can work with 50 neural network layers. The ResNet-50 model is divided into five stages, each with a convolution and identity block. Each convolution block has three convolution layers, and each identity block has three convolution layers as well. The ResNet-50 has over 23 million trainable parameters. whereas the EfficientNet is a convolutional neural network architecture and scaling method that uniformly scales all depth/width/resolution dimensions using a compound coefficient.

Here the test images are taken from the CoMoFoD dataset [11], that consist of 260 tampered examples. And for the analysis of the proposed model ,the F1-measure is calculated based on the confusion matrix. Table 1 shows the corresponding detection results.

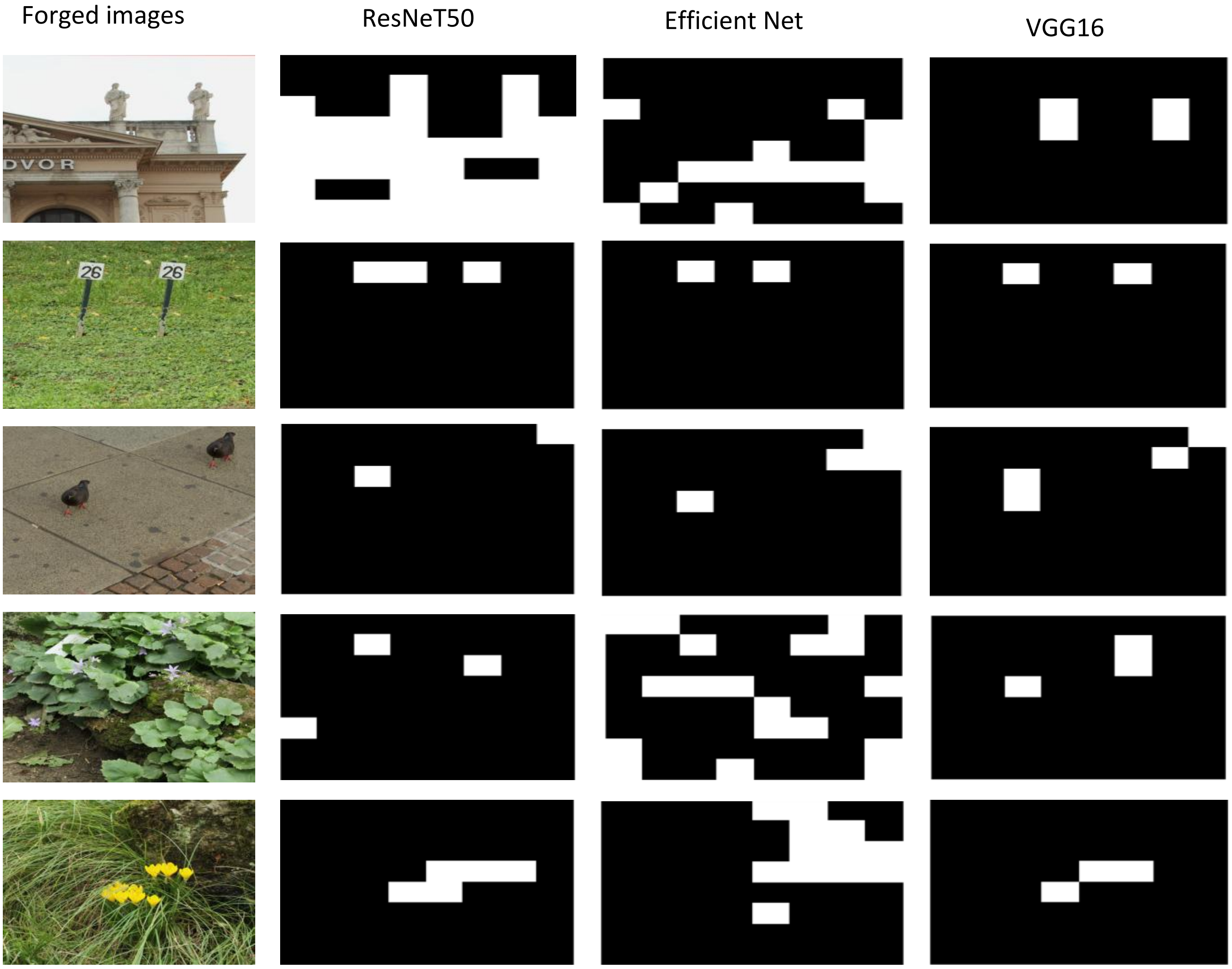

Fig -2 :The obtained results on some forgery examples

Table- 1: Detection Results

SL.NO	Method	Precision	Recall	F1- score
1.	ResNet50	0.841	0.077	0.142
2.	Efficient Net	0.208	0.05	0.080
3.	VGG16(Proposed Model)	0.506	0.456	0.480

It is also given the visual results of the proposed method with other two methods ie, ResNet50 and Efficient net. As a summary of the given visual results, it is clearly seen that our detection method detects forged regions more accurately than the other methods. The figure 2 shows the visual results of the proposed models with ResNet50 and the Efficient Net.

5. CONCLUSIONS

In this paper, deep learning-based framework is presented to detection and localization of copy move forgeries instead of using traditional feature extraction techniques. The method uses the VGG16 convolutional neural network to obtain image sub-blocks' features. After that, matching of them are realized with the Euclidean distance measure. Finally, evaluate the performance of the proposed method with two other methods(ie, ResNeT50, Efficientnet) using the F1- measure calculation. And it is proven with the test results that the proposed scheme is more successful than the other methods.

REFERENCES

[1] Fridrich, A. J., Soukal, B. D. and Lukáš, A. J., Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop (DFRWS), 2003.

[2] Popescu, A. and Farid, H., Exposing Digital Forgeries by Detecting Duplicated Image Regions, Tech. Rep., TR2004-515, Dartmount Collage, 2004.

[3] K. Sunil, D. Jagan, and M. Shaktidev, "DCT-PCA BasedMethod for Copy-Move Forgery Detection," Adv. Intell.Syst. Comput., vol. 249, pp. 577–583, 2014.

[4] N. Huang, J. He and N. Zhu, "A Novel Method for Detecting Image Forgery Based on Convolutional Neural Network," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1702-1705, doi: 10.1109/TrustCom/BigDataSE.2018.00255

[5] N. Hema Rajini, 2019, Image Forgery Identification using Convolution Neural Network, International Journal of Recent Technology and Engineering.

[6] S. S. Narayanan and G. Gopakumar, "Recursive Block Based Keypoint Matching For Copy Move Image Forgery Detection," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225658.

[7] K. Sunitha and A. N. Krishna, "Efficient Keypoint based Copy Move Forgery Detection Method using Hybrid Feature Extraction," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020, pp. 670-675, doi: 10.1109/ICIMIA48430.2020.9074951

[8] R. Agarwal, D. Khudaniya, A. Gupta and K. Grover, "Image Forgery Detection and Deep Learning Techniques: A Review," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 1096-1100, doi: 10.1109/ICICCS48265.2020.9121083.

[9] I. T. Ahmed, B. T. Hammad and N. Jamil, "Effective Deep Features for Image Splicing Detection," *2021 IEEE 11th International Conference on System Engineering and Technology (ICSET),* 2021, pp. 189-193, doi: 10.1109/ICSET53708.2021.9612569.

[10] Khudhair, Zaid Nidhal & Mohamed, Farhan & Abdulameer, Karrar. (2021). A Review on Copy-Move Image Forgery Detection Techniques. Journal of Physics: Conference Series. 1892.012010. 10.1088/1742-6596/1892/1/012010.

[11] D. Tralic, I. Zupancic, S. Grgic and M. Grgic, "CoMoFoD — New database for copy-move forgery detection," *Proceedings ELMAR-2013,* 2013, pp. 49-54.