Copy Move Forgery Detection Using CNN on Pre-Trained Model: BusterNet

Mayank Shrivastava[1], Arjun Singh[2], Ankit Singh[3], Dr. Farzil Kidwai[4]

[1, 2, 3] Student, Computer Science Department, Maharaja Agrasen Institute of Technology, New Delhi
[4]Assistant Professor, Computer Science Department, Maharaja Agrasen Institute of Technology, New Delhi

Abstract - With advancing technologies and plethora of editing tools it has become cumbersome to differentiate between real image and forged image. We introduce a Deep Neural Network for detecting passive image forgery. More precisely, this model is used for Copy Move Forgery Detection i.e. CMFD. Copy-move forgery in images is the most popular tampering method in which a portion of an image is copied and pasted in some other location of the same image. The architecture addresses two major limitations of older algorithms, firstly, it is end to end detection and secondly it produces source and target masks more accurately with varying threshold values. In recent years many models are being developed to detect forgery, In our model we have changed many existing things either by upgrading old data to newer version or by adding new technology to increase the efficiency of model. For example we will be using new libraries of Tensorflow and Keras to build whole model, also we will be adding some more data sets available publicly or from our side. We will change the pre existing values of data to newer one like standardization pixels of images from data set with the help of Convulational Neural Network. Experiment results are expected to change by developing new change in pre-existing model.

***Key Words*:** CNN, Image forgery, pixels, CMFD, CASIA, Data sets

1. INTRODUCTION

Image Forgery, which is defines as, “the process of cropping and pasting regions on the same or separate sources [10], is one of the most popular forms of digital editing. Copy Move Forgery Detection (CMFD) technologies are applied to find ‘clues’. A plethora of features are considered and required to detect copy-move forgery. Copy-Move image forgery with support of modern softwares has become enormously easy like Adobe, Vita etc., also mobiles have played a pivotal role in make fake images with free Applications available on Play store. Largely seen, the main goal of CMFD is to identify a probe image which contains cloned area, as an evidence to check any malicious intent. Based on classifications clone processes are generally of the three types which are *plain, affine* and *complex* forgeries.

Since, Busternet’s main functioning is end to end Deep Neural Network and also to produce different masks for source and target area in manipulated image. The model, for example, if two people are holding a rifle, model is not only interested in knowing about manipulation, but also making the clone i.e. different colour masks for source cone and target(manipulated area).

The key goal of our work is to optimize the process of detection of image forgery using Convolutional Neural Network (CNN), a domain of Machine Learning. The approach is towards the pre-trained existing BusterNet model architecture proposed by [1] on the publicly available datasets- CASIA v2.0 comprising of 3000 image sample sets and secondly CoMoFoD comprising of 260 image sets.

In our paper the main functioning of BusterNet was kept as original [1], we have tried to improve the capability of localizing and differentiating between the source and target clone. In original paper authors have used only 2626 image samples from CASIA out of 5000 total available, we instead will be taking all the images from CASIA around 4500 image samples. Also we will be upgrading the libraries like Keras and adding Tensorflow to model for improving the accuracy which is around 12 percent in the original paper. Also the main drawback of model was to image resizing limit to only 100x100 images at a time we will be resizing the images as 256x256.We aim to decrease the threshold values from 0.75 to 0.25 so that BusterNet can clearly make marks and hence improving its efficacy.

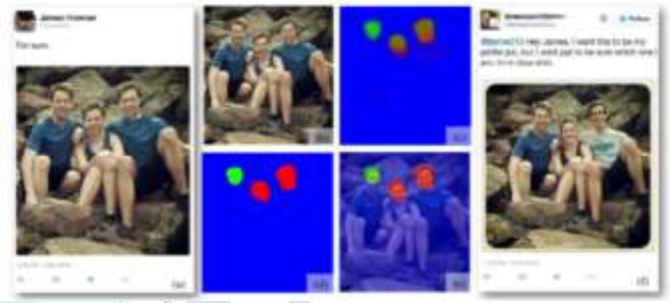

Fig.1. Whom in photo is not manipulated? BusterNet answers this question by not only detecting copy-move regions but also differentiating source (green) and target (red) copies. (a) tweet snapshot of a manipulated photo by James Friedman; (b) input region for analysis; (c) raw BusterNet output; (d) BusterNet output by applying majority rule; (e) overlaid result of (c) on (b); and (f) tweet snapshot of the original photo.

2. Literature Review

(Younis Abdalla, 2019) Detects copy move forgery using a fusion processing model which comprises deep convolution model and an adversarial model. In this paper four datasets are used. Experimental results show a high accuracy (95%) exhibited by the deep learning CNN and discriminator forgery detectors. Experimental results show an end to end trainable deep neural network approach for forgery detection appears to be optimal approach.

(Nam Thanh Pham, 2020) Propose an image forgery detection and localization algorithm that can handle both types of image forgeries simultaneously. The experimental results show that the proposed method outperforms state-of-the-art techniques in image forgery classification and localization accuracy. This paper introduces a novel method to detect and localize authentic images and two types of tampered images: copy-move and spliced images. The proposed algorithm determines the cluster centroid, which is the only authentic image in the cluster.

(Zaid Nidhal Khudhair, ILATOSPM 2020)Proposed an explanation to image forgery are introduced, and focused on copy-move image forgery detection. The review of many research papers on CMFD have been introduced in this paper which are published in reputed journals of from 2017 to 2020. In this many algorithms published (2017 to 2020) are presented and compared.

(Agarwal, 2020) Proposed approach is compared with some other existing techniques and results show that the proposed approach is better than the existing systems and effective even if the image is tempered by using various attacks. This paper uses deep learning feature extraction and matching algorithm. The SLIC method is used to extract features and ADM (Adaptive patch Matching) technique is applied to achieve the matched regions.

(Jigna J. Patel, Feb,2020) Proposed copy move forgery detection using CNN. It was proposed to overcome the limitations of block based and key point based classic methods for the copy move forgery detection. In this proposed method an end to end DNN pipeline is designed that is capable of achieving similar features from the tampered region wherein copied and source region have more similarity than those of other pristine region in the image. Evolution results of this method proves that this method is more robust than other copy move attacks and also detect various other forgeries that are not identified by state of the art algorithm to optimize the results LSTM can be combined with CNN approach.

(Somayeh Sadeghi, 2017) Discussed the advantage and drawbacks of state of the art algorithm in passive digital image forgery detection i.e. copy move forgery detection. Along with this various other forgery techniques have been discussed in this paper. The goal of this paper is to identified which copy move forgery detection technique are best for different image attributes like Scaling , rotation , JPEG compression. In the evolution result it was showed that key point based methods are much better than Block based method because of low computational time and better detection. The main drawback of existing copy moves forgery detection technique is that there is no way to find out the difference between copy move forgery and image retouching.

(Elaskily, Feb,2020)Tested an efficient, easy, fast Copy move forgery detection algorithm. For the above purpose this paper proposes deep learning method using CNN .it also decreasing the loss or misclassification of the copy move forgery. Based on deep neural learning a novel CMFD methodology is created. The experimental results showed that the proposed algorithm offers a very short TT compared with other algorithms. In future we can speed up the proposed algorithm using CNN modification.

2.1 OVERVIEW OF BUSTERNET

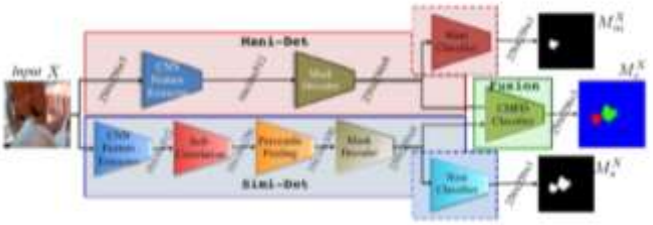

Fig.2 Overview of the proposed two-branch DNN-based CMFD solution. Dashed blocks are only activated during branch training. Output mask of the main task, i.e. $M^X{}_c$, is colour coded to represent pixel classes, namely pristine (blue), source copy (green), and target copy (red). Output masks of auxiliary tasks, i.e. $M^X{}_m$ and $M^X{}_s$, are binary where white pixels indicate manipulated/similar pixels of interests, respectively.

BusterNet follows two tier architecture having one branch name as Manipulation detection(Mani-det) and other one being Similarity Detection (Simi-det).Mani-det mainly focuses on detection of only manipulated region using standard CNN Extractor and standard Mask detector used widely in Convolutional Neural Networks. More precisely, it takes input image X, extracts features using CNN Feature Extractor, up samples the feature maps to the original image size using Mask Decoder, and applies Binary Classifier to fulfil the auxiliary task, i.e. producing a manipulation mask $M^X{}_m$. The manipulation detection branch (i.e. Mani-Det as shown by red shaded regions in Fig. 2) can be thought of as a special segmentation network whose aim is to detect manipulated regions.

The similarity detection branch (i.e. Simi-Det as shown by blue shaded regions in Fig. 2) takes an input image X, extracts features using CNN Feature Extractor, computes feature similarity via Self-Correlation module, collects useful statistics via Percentile Pooling, up samples feature maps to the original image size using Mask Decoder, and applies Binary Classifier to fulfil the auxiliary task, i.e. producing a copy-move mask MX m at the same resolution of X. (Yue Wu W. A.-A., 2018)

3. PROPOSED METHODOLOGY:

In original model, the authors have used python 3.0 version for programming and developing of the model BusterNet back in 2018, but now in current time python upgraded its version to 3.9.1 so while developing the model we also upgraded various libraries to cope up with upgraded python version like numpy, matplotlib etc. libraries.

The following points explain:

(i) In original model authors have used Keras library but this library version of 2.0.7 is now outdated, we will use latest version of 2.4.3, but Keras simultaneously need Tensorflow library as a backend so as a result we will be upgrading Tensorflow from outdated version of 1.1.0 to newer version of 2.5.0.

(ii) Furthermore, the main model functioning will be kept as it was except some minor changes as (i) leading to minor change.

(iii) In older model only 1313 image sets (i.e. 2626) were only used form dataset CASIA V2.0 and that too with the manipulation of the authors but we will we taking into account approximately all the images of dataset CASIA v2.0 and also we will be taking newer version of CoMoFoD dataset which has 260 forger image sets as compared to 200 image sets used in the authors model.

(iv) Moreover, we have proposed to increase the fixation of resolution of images of dataset. Previously, fixation of image was restricted to 100X100 from which we will be taking it into 256X256 which will incur less loss of information during resizing and also the discerniblity of BusterNet will, it will make more accurate masks in Semi-det and Mani-det branches and eventually in direct use of model and increasing the efficacy.

In older model authors have trained model with Microsoft's COCO data set but we will not go into details for more details refer them: (Younis Abdalla, 2019), (Yue Wu W. A.-A., 2018), (Yue Wu W. A., 2019).

Coming into main role, the original model had accuracy of only approximately 12 percent we aim to optimize direct fusion model of BusterNet of differentiating source and target clone in the manipulated images by 4-5 percent by using above points. It was also seen that Synthetic data was used previously but we aim to more of other data possibly like USC-ISI (small) comprising of 100 images and picking up randomly to test the model differentiation.

4. EXPERIMENTATION AND RESULTS:

This section presents the implementation of the proposed approach using the hardware as Intel(R) Core™ i7-5500U CPU with 2.40 GHz, 6 GB RAM and software as Windows 10 with python release 3.9.1 and compared the proposed approach with the existing state-of-the-art approaches. According to our proposed method we first updated the datasets discretion given in 5.1. Then for testing images we made the changes in 5.2 as Baseline settings and Overall Performance of BusterNet in 5.3 and most importantly Busternet's Discernablity of Source/target copies in 5.4.

4.1 DATA SET

We use two standard datasets for evaluation. The first dataset is the CASIA TIDEv2.0 dataset, which is the largest public accessible image forgery detection benchmark, in which all manipulations are created manually. It contains 7491 authentic and 5123 tampered colour images. However, it does not specify which images are manipulated in a copy-move manner and does not provide ground truth manipulation masks. We therefore verified 4500 out of 5123 tampered samples are of copy-move forgery. These 4500 CMFD samples and their authentic counterparts together form the testing dataset (total 9000 samples) we used later. We refer to it as the CASIA CMFD dataset. The second dataset is the CoMoFoD dataset (Yue Wu W. A.-A., 2018), which in original contained 200 image sets and now which has been upgraded to 260 base forged images and 25 categories (total 6500 images). Each category is made by applying post processing/attacks to the base category images to hide forgery clues (e.g., JPEG compression, etc.). Detailed attack descriptions and settings can be found in (Tralic, 2013).

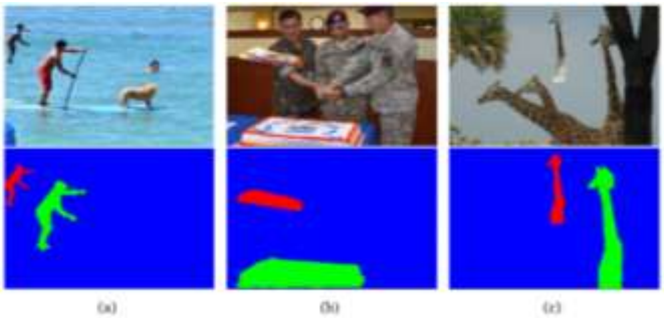

Fig.3 Images and their masks of Data Set

4.2 BASELINE SETTINGS OVERVIEW

We use precision, recall and F1 scores to report CMFD performance as authors have done. For a testing image, we compute the true positive (TP), false positive (FP) and false negative (FN) at pixel level. Of course, we have to treat pixels classified to source and target both as forged, so that the proposed BusterNet could be fairly compared with all classic CMFD methods which only predict binary masks. We changed the resolution of images from 100X100 fixed resizing to 256X256 resizing. Based on how F1 is calculated, two protocols are used for pixel-level evaluation:

(A) Aggregate all TP, FP, and FN numbers over the whole dataset, and report precision, recall and F1 scores and;
(B) Compute precision, recall, F1 scores for each image, and report the averaged scores.

Protocol A better captures overall performance including non-forged images, while protocol B only works for a subset of forged images (F1 score is ill-defined when TP is zero), but better quantifies the localization performance. We use both protocols in our evaluations. If any pixels in a testing image are detected as forged, the testing image is labelled as forged. We compare a predicted image label with its ground truth to compute image-level TP, FP, and FN, and report precision, recall and F1 scores over an entire dataset as image-level evaluation protocol.

4.3 OVERALL PERFORMANCE

	Authors		Ours	
	Simi.- Det.	BusterNet	Simi.- Det.	BusterNet
	Image Level Evaluation Protocol			
Precision	71.53	78.22	72.91	79.42
Recall	80.73	73.89	80.73	74.76
F-Score	45.85	75.89	45.85	78.76
	Pixel Level Evaluation Protocol-A			
Precision	56.52	77.38	57.01	77.38
Recall	62.06	59.15	63.45	59.15
F-Score	59.16	67.05	59.96	67.05
	Pixel Level Evaluation Protocol-B			
Precision	47.23	55.71	46.03	59.8
Recall	48.44	43.83	49.11	47.6
F-Score	43.72	45.56	41.09	48.9

Table 1.Performance analysis on CASIA CMFD dataset

There is a slight improvement in Image level Protocol as well as Pixel Level Protocol between Authors and ours but there is an improvement of around percent in Pixel Level Evaluation, with the change of libraries and with bigger database we have slightly improved the Overall performance of Busternet.Since Protocol A takes average value of all images the total remains same hence no improvement is seen but in protocol each image is taken into consideration and hence a wider range is tested leading to improvement in the model. As shown below in the figure 4.

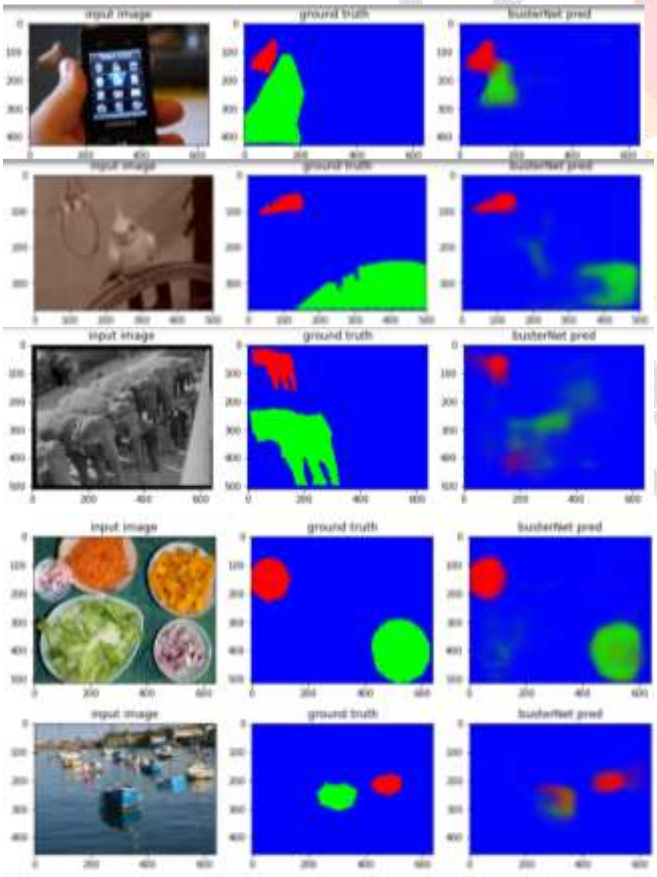

Fig.4 Implementation and overall performance of BusterNet

4.4 BUSTERNET'S DISCERNABLITY OF SOURCE/TARGET COPIES

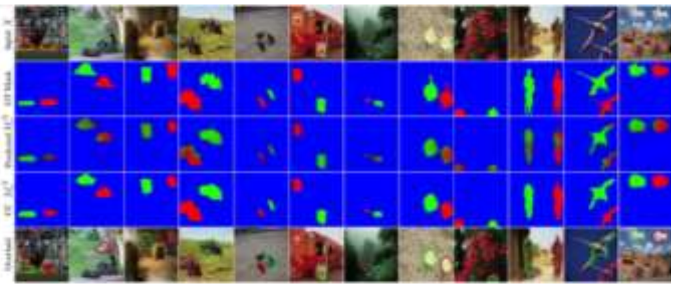

Fig.5 BusterNet detection results on testing dataset. Samples that BusterNet correctly distinguishes source/target copies; blue: pristine, green: source copy and red: target copy

The main goal of the paper to improvise the BusterNet model greater than 12 percent was achieved. Many object classes, e.g. flower, sand, and ladybug, which were not included; indicating the generalizability of BusterNet to unseen classes has been improved. In order to evaluate the accuracy of localization, we compare the predicted forgery region labels with those from ground truth. For each predicted mask, we merge the source and destination channels to find all forged regions using the connected component (CC) analysis, and use the dominant class of all its pixels as the label of a CC.The different classes of images as follows:

(I)If no CC is found, this is a miss.

(II)If all CCs in a sample have the same label, we opt-out this sample.

(III)Otherwise, this is an opt-in sample for analysis, and we label it “correct” only when both source and target forgery regions are correctly classified.

Visual examples are shown in Fig.5 and Table 2 summarizes the discerniblity performance of BusterNet on both the CASIA CMFD and CoMoFoD datasets, where miss indicates those missed samples, overall accuracy is the ratio of corrected samples to total samples, and opt-in accuracy is the ratio of corrected samples to opt-in samples.

The overall 18% accuracy does not seem that high. However, one should consider the fact that BusterNet is only trained with synthetic data with a limited number of real manipulation samples, and the used simple CC-based label assignment scheme is also simple for complicated real cases and only two datasets are used if other datasets like MICC are used with different kinds of passive forgeries then the accuracy will surely improve. As one can see in Fig.5 BusterNet correctly captures target manipulation at least partially (e.g., the left-most bird sample and the right-most spider sample), but the simple CC-based label scheme fails to assign correct labels. Indeed, if we consider the accuracy only for opt-in samples, since they are only TRUE POSITIVE the accuracy of the proposed BusterNet jumps to around ~81% as shown in Table 2.

	Number of Images					Accuracy	
Dataset	**Total**	**Miss**	**Opt-out**	**Opt-in**	**Correction**	**Overall (In %)**	**Opt-in**
CASIA CMFD	4500	1395	1400	950	761	16.10	80.10
CoMoFoD	200	58	81	61	52	19.15	85.33
Overall	4700	1453	1481	1011	813	17.29	80.41

Table 2.Source and Target discerniblity performance of BusterNet.

5. CONCLUSIONS

This paper proposed an image forgery detection approach using CNN based pre trained BusterNet model to extract deep features, with less time investing in training of model. Two-tier based architecture was upgraded with latest technologies and libraries. The performance of BusterNet is increased overall by approximately 4 percent in all three i.e. precison,F1 and recall pixels on CASIA dataset, but on the contrary performance of BusterNet remained around same as the author even after taking more image sets if images. The discerniblity of BusterNet has been significantly improved on both the date sets; Overall accuracy of 16.1 percent was achieved by taking around all the samples of CASIA and CoMoFoD and "opt-in" accuracy is achieved at 80.1 percent. It is quite successful on positive images (already manipulated) but with synthetic manipulation. The BusterNet in future can be used in Image forensics may be by changing the resolutions of images to higher values. Although model has still some limitations but with advancing Deep leaning algorithms it can be more improvised. As it outcomes most of the sate-of-art methods for CMFD and if more non synthetic data used and out of domain images, its ability of distinguishing between source and target copies of image clones is desired capability of forensics experts.

REFERENCES

Abdalla, Y. &. (2019). Convolutional Neural Network for Copy-Move Forgery Detection. *Symmetry. 11. 1280. 10.3390/sym11101280.*

Agarwal, R. &. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. . *Multimedia Tools and Applications. 79. 10.1007/s11042-019-08495-z.* .

Amit Doegar, M. D. (2018). CNN based Image Forgery Detection using pre-trained AlexNet Model. *International Conference on Computational Intelligence & IoT (ICCIIoT)*, (pp. 402-408).

Bhavasar, A. K. (Feb,2020). Syn2Real: Forgery Classification via Unsupervised Domain Adaptation. (p. 8). IIT Mandi.

Chao Yang, H. L. (2020). CONSTRAINED R-CNN: A GENERAL IMAGE MANIPULATION DETECTION MODEL. *IEEE* (p. 6). International Conference on Multimedia and Expo (ICME2020).

Elaskily, M. E. (Feb,2020). A novel deep learning framework for copy-moveforgery detection in images. *Multimed Tools Appl 79* , 19167–19192.

Jessica Fridrich, D. S. (2019). Detection of Copy-Move Forgery in Digital Images. *Air Force Material Command [F30602-02-2-0093]*.

Jigna J. Patel, N. S. (Feb,2020). Copy-Move Forgery Detection in Digital Images using Neural Network. (pp. 1560-1564). Blue Eyes Intelligence Engineering.

Nam Thanh Pham, J.-W. L.-S. (2020). Structural Correlation Based Method for Image Forgery Classification and Localization.

Rajini, N. H. (June,2019). Image Forgery Identification using Convolution Neural Network. *International Journal of Recent Technology and Engineering (IJRTE)*, (pp. 311-320).

Somayeh Sadeghi, S. D. (2017). State of the art in passive digital image forgery detection: copy-move image forgery. *Pattern Analysis and Applications* .

Tralic, D. Z. (2013). Comofodnew database for copy-move forgery detection. *ELMAR, 2013 55th international symposium*. (pp. 49–54). IEEE.

YEW, Y. Y. (2018). *IMAGE FORENSIC FOR DIGITAL IMAGE COPY MOVE FORGERY DETECTION* . Malaysia.

Younis Abdalla, M. T. (2019). Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network. 26.

Yue Wu, W. A. (2019). ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)* , 9543-9552.

Yue Wu, W. A.-A. (2018). *BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization*. ECCV.

Zaid Nidhal Khudhair, D. F. (ILATOSPM 2020). A Review on Copy-Move Image Forgery Detection Techniques. *Journal of Physics: Conference Series* .