A Comparative study of State of Art Methods and Deep learning networks for detection of copy-move forgery in digital images

Jigna J. Patel[1] & Dr.Ninad S.Bhatt[2]

Gujarat Technological University, Chandkheda, Ahmedabad, Gujarat, India[1],
C.K.Pithawala College of Engineering and Technology, Surat, Gujarat, India[2]

jigna2012me@gmail.com[1], ninad.bhatt@ckpcet.ac.in[2]

Abstract: *In today's scenario, all the software applications for editing or enhancing images are easily available. As a result of which it has become common to enhance an image, moreover tempering of an image has become very easy and hence, the integrity of the image is compromised. In order to preserve the authenticity of an image, it is necessary to develop some algorithms to detect forged regions of an image, if there is any. There exist , two state-of-art methods for detection of digital image forgery: the key- point based method in which major key points of the image is found and forged part is detected and the block based method that locates the forged part by sectioning the whole image into blocks. Unlike these two classic methods that require multiple stages, there exists a better solution -the deep learning architecture Convolutional Neural Network which provides a better option for extraction of forged regions. Proposed work revealed a better forgery detection performance than any other classic approaches.*

Keywords: **Copy-Move forgery detection; Convolution Neural Network; SIFT, Pixel-Based Image Forgery Detection, Block Based Image Forgery Detection**

1. INTRODUCTION

In today's life, all the tools which can damage the authenticity of an image are easily available. Most of which we get free as an application of mobile phones. Due to this, anyone can easily temper the image by hiding some portion or by pasting some other part of image into one image. These fake images can further be used for forensic purpose or utilized by newspaper editor to be published in the newspaper. In such a case, authentication of an image is a must. There are several ways to temper an image which includes removal or replacement of some parts of the digital image or creation of one image from various images known as image splicing. Copy-Move Forgery is one such method to temper an image in which portion of the same image is copied and pasted in the same. This copied part before pasting can be geometrically transformed or some post-processing operations, such as rotation, scaling, JPEG compression, noise addition, etc., may be done before pasting. But one cannot make out the copied portion with human eyes as the tempered region is similar in terms of color and texture to the original one. Many algorithms exist which detects copy-move forgery. Among them state-of-art methods are: block-based and key-point based techniques. Block-based methods extract features from overlapping blocks of the image and key-point based method extract the points of interest from the whole image. But recently, deep learning approach became much more popular for the detection of various types of forgery that includes scaling rotation of a copied part and pasting in the image or a combination of multiple forgeries.

2. RELATED WORK

In general, the framework of copy-move forgery detection consists following steps and is given as follows:

a. The first step in CMFD is generally pre-processing that converts the image into gray scale image which is then resized.

b. As the second step, feature extraction is carried out into which the image is usually converted into a set of features of interests.
c. After feature extraction, feature matching is carried out wherein the similarity or distance between two features is measured and; finally,
d. Post- processing to further improve the detection of forged part that includes the use of a set of heuristics, which reduces the rate of false alarms and to improve the number of true positives.

Further, CMFD can be classified as key-point based methods which comprises of SIFT [8,9], ORB [10,11], SURF [12,13], and irregular region-based methods [14,15] and block based approaches, that includes various research works in Polar harmonic transform [1], PCA feature [2,3], Zernike moments [4,5], DCT [6,7]. Each and every method has its own advantages as well as drawbacks for detection of Copy-Move Forgery. For instance, key-point based methods are fast and robust against affine transformation but they often fail to identify the forged areas when copied and pasted regions are homogeneous. On the contrary, the block-based methods, even though simple, are computationally expensive. Even though, both methods have its own advantages and disadvantages; however key-point based methods may not be suitable for copied smooth regions, whereas block-based methods work well in such cases, yet, it will bring high computation cost.

In the recent years, Convolutional Neural Network (CNN) is a well-known deep learning architecture, and is a great success in the task of image forgery detection. In the digital image passive forensics field, many researchers contributed to research by CNN. For instance, in [16], the authors introduced a new end-to-end deep neural network, which was robust against several assaults. Meanwhile, in [17], the authors utilized deep neural network for extracting features on behalf of the copy-move forgery identification. Later, in [18], authors used a DNN-based patch classifier for the recognition of counterfeited regions. Furthermore, in [19], the authors proposed an end-to end DNN for splicing detection and localization. In [24] Kang et al., first applied the CNN into the median image filter forensics.In [25], Baroffio et al.applied it into camera type identification of image forensics. In [26], Belhassen et al. proposed a general model of image tampering. In [27], Xu et al. used CNN to the image steganography analysis. Inspired by these works; we will explore the application of image copy-move forgery detection by the CNN.

3. METHODOLOGY

3.1 Overview

To design an end-to-end CNN network architecture that is capable of giving the forged region as an output, we design a Deep Neural Network such that it does not include manually tuned parameters and is capable of producing distinct source and target manipulation masks (which could also be useful for forensic analysis). Consequently, as inspired by [20], we proposed a deep neural network architecture that is capable of distinguishing all types of tempered regions, which has undergone various transformations before forgery. The proposed DNN architecture is as shown in Fig. 1. It will be explained in detail in sections below.

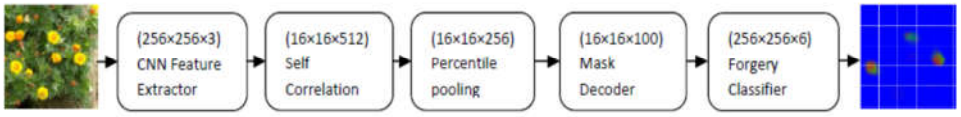


Figure.1. Overview of the proposed DNN-based CMFD solution

3.2 CNN Feature Extractor

Compare to the traditional CMFD approach, like block-based CMFD or key-points based CMFD, the resulting CNN feature identifies the appropriate feature representations for the image copy-move forgery detection problem from training the data automatically. The primary concern of using the convolutional feature extractor is to extract block-like features for a given image. We use VGG16 CNN feature extractor [23] for extracting features from an image. We had utilized convolution and max-pooling layers in the first four blocks of the VGG16 model. If we input image X of size 256 × 256 × 3, we get as an output, a feature tensor f_s^X of size 16 × 16 × 512 from the VGG16 convolutional feature extractor.

3.3 Clone Detection

With the help of CNN Feature Extractor, the Clone detection branch starts with feature representation. Further, it produces a feature tensor f_s^X of size 16×16×512, which can be seen as 16×16 patch-like features, i.e.$f_s^X = \{f_s^X [ir, ic]\}$ ir, ic [0… 15], each with 512 dimensions. Since we want to locate the cloned/forged regions, there was the need to search for useful information in order to decide what the matched patch-like features are. To achieve this, all-to-all feature similarity score was calculated using Self-Correlation, and then, meaningful statistics were obtained to identify matched patches via Percentile Pooling. Given the two patch-like feature $f_m^X[i]$ and $f_m^X[j]$ where i= (ir, ic) and j = (jr, jc), the Pearson correlation coefficient ρ was used to calculate the feature similarity as shown in Eq. (1)

$$\rho(i, j) = \left(\check{f}_m^X[i]\right)^T \check{f}_m^X[j] /512 \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

where (.)T is the transpose operator, and $\left(\check{f}_m^X[i]\right)$ is the normalized version of $f_m^X[i]$ and it is shown in Eq. (2)

$$\check{f}_m^X[i] = \left(f_m^X[i] - \mu_m^X[i]\right) / \sigma_m^X[i] \quad \ldots\ldots\ldots (2)$$

where $\mu_m^X[i]$ is the mean and $\sigma_m^X[i]$ is the standard deviation.
We repeat the process over all possible $f_m^X[j]$, for a given $f_m^X[i]$, and in this manner form a score vector $S^X[i]$, namely

$$S^X[i] = [\rho(i, 0), \cdots, \rho(i, j), \cdots, \rho(i, 255)] \ldots. (3)$$

As an output from Self- Correlation, a tensor SX of shape 16×16×256 was produced. Hereafter, the Percentile Pooling was employed, which first sorted the score vector SX[i] to S′X[i] in a descending order, wherein the sorted vector depicted an abrupt drop at some point which can be used to decide on the feature matching. After getting the resultant tensor from Self-Correlation Percentile Pooling first sorts a score vector SX[i] to S′X[i] in the descending order as shown Eq. (4).

$$S'X[i] = \text{sort}(SX[i]) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Using this sorted score; one can decide what feature is matched. However score vector has a drawback i.e. its length is dependent on the input size.

Taking this into consideration, Percentile Pooling was used to remove this dependency and standardize the sorted score vector through selecting those scores at the percentile ranks of interests. Also, the Percentile pooling aids in reducing the dimensions, as it keeps only a small portion of all scores. After that, we use the Mask Decoder to gradually up sample feature PX to the original image size as d_s^X. Finally, Binary Classifier produced a copy-move mask M_s^X which is used to predict the similarity between two forged regions, which is as simple as a single Conv2D layer with 1 filter of kernel size (3,3) followed by the softmax activation.

All the other modules are either standard or can be fabricated from standard layers except Self-Correlation and Percentile Pooling modules. For Self-Correlation, implementation of Eqs. (1) and (2) was required. On the other hand, Percentile Pooling was just a pooling layer, which had no trainable parameters but only a deterministic pooling function. Therefore, backpropagation was conducted similar to the one performed in standard MaxPooling in which only the neuron corresponding to the max receives the gradient.

3.4 Forgery Classifier

The output of the classifier that activated during the training period was the cloned regions that are manipulated. It was, then, assumed that the input image X was of size 256×256×3. We extract features from the image X using CNN Feature Extractor and the similarity between features was calculated using Self-Correlation module and lastly, collected useful statistics through Percentile Pooling. Next, by the use of the Mask Decoder, the feature map was unsampled to its original image size and finally, binary classifier was initiated to produce a copy-move mask M_s^X at the same resolution of the input image.

We made the use of Adam optimizer and binary crossentropy loss function. Whenever validation loss reaches plateaus after 10 epochs, we reduce learning rate by half until improvement stops for 20 epochs.

4. EXPERIMENTAL RESULTS AND DISCUSSION

For training, initialization of all the parameters were done using weights from a pre-trained model, which was taken from [20], the VGG16 on ImageNet for CNN Feature Extractor in Clone detection section. For the primary task, the Adam optimizer with categorical cross entropy loss was used. At the same time, precision, recall and F1 scores were collated in order to account the CMFD's performance [20]. For the testing purpose, four values were computed: true positive (TP), true negative (TN), false positive (FP) and false negative (FN). Subsequently, the computation of precision, recall, and F1 scores was accomplished for evaluating the overall performance of the network. The CoMoFoD dataset [21], which contains 200 base forged images and 25 categories (total 5000 images), was used to check the overall performance of the network. To conceal the falsification in the image each category was made by applying post-processing or attacks to the original image category. The overall description of the attacks and settings in detail can be found in [21]. Finally, the data were evaluated using ground truth masks, thereby, distinguishing the forged part from the pristine regions so as to analyze the network's degree of discernibility.

Table 1, as presented below, illustrates the overall performance based on the CoMoFoD dataset.

Table.1 Overall performance on CoMoFoD Dataset

	CoMoFoD Dataset *(Image Level Evaluation Protocol)*	
	Proposed Work	SIFT

Precision	73.65	68.32
Recall	72.9	66.71
F1 Score	99	67.50

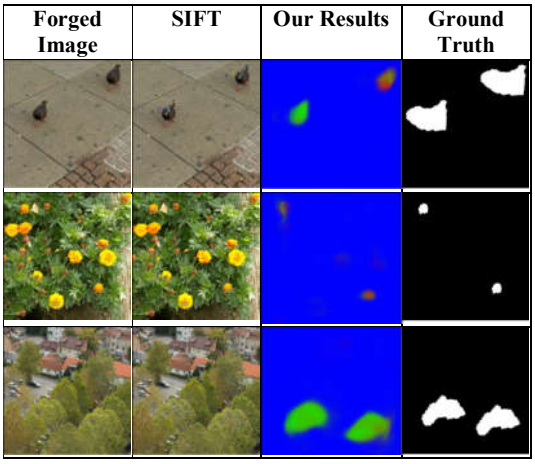
From the table above, it can be concluded that in comparison to the state of art method using SIFT algorithm [28], the experimental results of the proposed network showed a better accuracy of 73.65% over the CoMoFoD dataset.

For the evaluation of the network's robustness against several assaults or post-processing, it was tested against the CoMoFoD dataset as shown in Table 1, while the total number of correctly detected images, which underwent five different attacks and contained 200 samples each, is presented in the Table 2. An image is considered as correctly detected if it's pixel-level F1 score is higher than 0.5 [22]. Hence, based on the evaluation of the network performance, the system is quite robust for the detection of various forgery attacks for all images. The overall performance of the CNN model in comparison to SIFT is also summarized in Table 2. Moreover, the proposed network reflected a 73.65% overall accuracy.
The total Images correctly detected according to the Image Type is shown in the table below:

Table.2 Performance analysis based on the Image Forgery type

Image Type	Total Correctly Detected	Image Type	Total Correctly Detected	Image Type	Total Correctly Detected
BC1	115	NA3	102	JC2	77
BC2	114	CA1	118	JC3	85
BC3	110	CA2	116	JC4	102
CR1	116	CA3	115	JC5	98
CR2	117	IB1	111	JC6	100
CR3	115	IB2	103	JC7	106
NA1	99	IB3	94	JC8	108
NA2	101	JC1	61	JC9	105

The results of our experiment based on the Image Forgery type are shown in Figure 3.



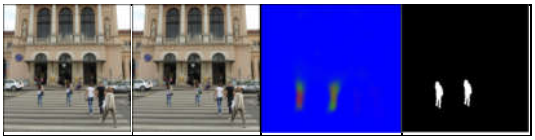


Figure 3. Comparison of SIFT and Proposed Work

5. CONCLUSION and FUTURE WORK

In this paper, we proposed an end-to-end CNN solution for detecting of forged regions in an image. Our experimental results demonstrated that our method was robust against various known Copy-Move attacks, and also detects several types of forgery that cannot be identified by state-of-the-art algorithms. Hence, this approach can be further optimized for different types of forgeries like image splicing detection, etc. Also, we can have a combined approach of LSTM with CNN to further optimize the results.

REFERENCES

[1] *Li L, Li S, Zhu H, Wu X. "Detecting copy-move forgery under affine transforms for image forensics", Computers & Electrical Engineering , Vol.40, Issue 6,Elsevier'**(2014),** pp. 1951-1962.*

[2] *Huang, D.Y., Huang, C.N., Hu, W.C., Chou, C.H.: Robustness of copy-move forgery detection under high jpeg compression artifacts. Multimedia Tools and Detection Applications 76(1), **(2017),** pp. 1509–1530.*

[3] *Alaa Hilal, Taghreed Hamzeh, Samer Chantaf,"Copy-move forgery detection using principal component analysis and discrete cosine transform", Sensors Networks Smart and Emerging Technologies (SENSET)-IEEEXplore,**(2019)***

[4] *Seung-Jin Ryu, Min-Jeong Lee, Heung-Kyu Lee,"Detection of Copy-Rotate-Move Forgery Using Zernike Moments", Springer ,Information Hiding **(2010)**, pp 51-65.*

[5] *Mahmood, T., Nawaz, T., Irtaza, A., Ashraf, R., Shah, M., Mahmood, M.T.: Copy-move forgery detection technique for forensic analysis in digital images. Mathematical Problems in Engineering **(2016)**, pp 1-13.*

[6] *Ashima Gupta, Nisheeth Saxena, S.K Vasistha,"Detecting Copy move Forgery using DCT" ,International Journal of Scientific and Research Publications, Volume 3, Issue 5,**(2013)**,pp-1-4.*

[7] *Hesham A. Alberry,Abdelfatah A. Hegazy, GoudaI Salama," A fast SIFT based method for copy move forgery detection", Future Computing and Informatics Journal**(2018)**, pp-159-165.*

[8] *Yang, B., Sun, X., Guo, H., Xia, Z., Chen, X.: A copy-move forgery detection method based on cmfd-sift. Multimedia Tools and Applications**(2017)**, pp. 1–19.*

[9] *Rajdeep Kaur, Amandeep Kaur,Copy-Move Forgery Detection Using ORB and SIFT Detector,Volume 4, Issue 4,IJEDR**(2016)**, pp-804-813.*

[10] *Zhu, Y., Shen, X., Chen, H.: Copy-move forgery detection based on scaled orb.Multimedia Tools and Applications 75(6), **(2016)**, pp 3221–3233.*

[11] *Guang-qun Zhang,Hang-jun Wang,"SURF-based Detection of Copy-Move Forgery in Flat Region", International Journal of Advancements in Computing Technology(IJACT),Volume4, Number17,* ***(2012)****, pp-521-529.*

[12] *Silva, E., Carvalho, T., Ferreira, A., Rocha, A.: Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. Journal of Visual Communication and Image Representation 29,* ***(2015)****, pp 16–32.*

[13] *Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detection scheme. IEEE Transactions on Information Forensics and Security 10(3),* ***(2015)****,pp 507–518.*

[14] *Pun, C.M., Yuan, X.C., Bi, X.L.: Image forgery detection using adaptive oversegmentation and feature point matching. IEEE Transactions on Information Forensics and Security 10(8),* ***(2015)****,pp 1705–1716.*

[15] *Yue Wu, Wael Abd-Almageed, and Prem Natarajan, "Image Copy-Move Forgery via an End-to-End Deep Neural Network", Winter Conference on Applications of Computer Vision, IEEE'****(2018)****,* pp 168-184*.*

[16] *Liu, Y., Guan, Q., Zhao, X.: Copy-move forgery detection based on convolutional kernel network. Multimedia Tools and Applications,* ***(2017)****, pp. 1–25.*

[17] *Bunk, J., Bappy, J.H., Mohammed, T.M., Nataraj, L., Flenner, A., Manjunath, B., Chandrasekaran, S., Roy-Chowdhury, A.K., Peterson, L.: Detection and localization of image forgeries using resampling features and deep learning. In: Computer Vision and Pattern Recognition Workshops (CVPRW),* ***(2017)*** *,pp. 1881–1889..*

[18] *Wu, Y., Abd-Almageed,W., Natarajan, P.," Deep matching and validation network: An end-to-end solution to constrained image splicing localization and detection", Proceedings of the ACM on Multimedia Conferenc,* ***(2017)****, pp. 1480–1502.*

[19] *Wu, Yue, and AbdAlmageed, Wael and Natarajan, Prem," BusterNet: Detecting Image Copy-Move Forgery With Source/Target Localization", European Conference on Computer Vision (ECCV)Springer,****(2018)****.*

[20] *Dijana Tralic, Ivan Zupancic, Sonja Grgic, Mislav Grgic: Comofodnew database for copy-move forgery detection. In: ELMAR, 2013, 55th international symposium,****(2013)****, pp.49–54.*

[21] *Tralic, D., Zupancic, I., Grgic, S., Grgic, M.: Comofodnew database for copy-move forgery detection. In: ELMAR, 2013 55th international symposium,* ***(2013)****, pp. 49–54.*

[22] *Simonyan K., Zisserman A,"Very deep convolutional networks for large-scale image recognition",* ***(2014)****.*

[23] *J. S. Chen, X. G. Kang, Y. Liu, and Z. J. Wang, "Median Filtering Forensics Based on Convolutional Neural Networks,"IEEE Signal Processing Letters, vol. 22, no.11,****(2015)****, pp. 1849-1853.*

[24] *L. Baroffio, L. Bondi, P. Bestagini, and S. Tubaro,"Camera identification with deep convolutional networks,"****(2016)****.*

[25] *B. Bayar, "A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer," Acm Workshop on Information Hiding & Multimedia Security,* ***(2016),*** *pp.5-10.*

[26] *G. S. Xu, H. Z. Wu, Y. Q. Shi. Structural Design of Convolutional Neural Networks for Steganalysis[J]. IEEE Signal Processing Letters, vol. 23, no.5,* ***(2016),*** *pp. 708-712.*

[27] *Christlein V.,Riess C., Jordan J., Riess C., Angelopoulou E.," An evaluation of popular copy-move forgery detection approaches", IEEE Transactions on information forensics and security 7(6),* ***(2012)****, pp. 1841–1854.*