CMFD using a Novel Localisation Technique and CNN based Classification

Ritu Agarwal, Om Prakash Verma

Abstract*: Latest trends of the image processing software, the growth of image manipulation is at peak. To detect the use of such software on an image is a growing research anomaly. This paper proposes a novel copy-move forgery localization approach in an image through a blind approach with no prior information available to the algorithm. Here, we have split the image into equal size blocks and extracted SIFT features for every block. The center of mass for each block is calculated after applying the Gaussian filter. Finally, image features are matched based on the KNN algorithm for CMF localization. However, for classification, the localisation mask is created for the dataset, and is used to train a Convolutional neural networks(CNN) and this trained CNN in turn is used for classification of images as authentic or tampered.

***Keywords*: Image Forgery, Copy move forgery detection, Convolutional Neural Network, Image Segmentation, SIFT.**

I. INTRODUCTION

Digital Image forensics, a study of image authentication. An image implies the truth of what it represents. With the emergence of digital media, namely images and the comparative ease of processing them, the originality and integrity of an image are uncertain. Tools invented and used for improving information on a digital image, are being used for doctoring them and also for personal as well as professional benefits. Tampering can be, in such a way that the naked eye cannot perceive it. Tampered images nowadays find their place in every aspect of society. It can be news reports to create havoc among the masses, or for business/marketing for professional benefits by defaming the competitor, the court of law for attacking or defending criminal/non-criminal acts, military affairs, academic research, medical research, etc. Numerous examples can be found everywhere, of such destructive actions. Therefore, there is a neverending need for detection of such acts of forgery which can keep us update with the technological advancements in this area.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Ritu Agarwal*, Assistant Professor,Department of Information Technology ,Delhi Technological University,(formerly Delhi College of Engineering), Delhi India
Om Prakash Verma, Assistant Professor,Department of Electronics and Communication Engineering, Malaviya National Institute of Technology, Jaipur, India.

Image forgery methods are mostly categorised into Copy Move, Image Splicing/Photomontage, and Image Retouching [1]. Copy Move Attack is a commonly used image forgery technique which can distort the integrity of an image. Distortion in images here may mean to hide some part of the information or reveal extra information. In this attack, a section of an image is replicated elsewhere in that very image [2]. Image Splicing also known as Photomontage is a tampering technique where an image is manipulated by merging parts of two images and creating a third image[3]. Image Retouching or Image Brushing is another tampering technique where a part of an image or the complete image is enhanced in order to highlight a particular trait. This type of forgery is mostly done in magazines or modeling domain where the subject is highlighted to make it captive[4]. This paper proposes a novel technique to localize the Copy Move Forged area as shown in Fig. 1. The center of mass helps in concentrating the keypoints on the gradient image, at the copy-moved areas. The localisation mask thus created in turn is used to train a Convolutional Neural Network. The trained network can be used to classify an image or a set of images from a datatset as forged or authentic. Though most of the machine learning based CMFD approaches describe the training of network through mask images of the forged image. However, in most cases those mask images are not available to properly train the network efficiently. In order to achieve an accurate network which detects the forged region comprehensively require plethora of image masks. In this paper, we have proposed a blind image approach which can create a forged image masks to train our designed neural network precisely. This paper is divided into five sections. After an introduction to the objective of the paper in Section I, related work with similar objectives as the paper is discussed in Section II. Proposed approach is discussed in section III which has further subsections explaining the work in detail, followed by results and discussion in section IV and a conclusion as to how the objective is achieved is stated in section V.

II. RELATED WORK

Image tampering detection has taken its toll in many a literature. Wu et al. extract block like features from an image by using a convolutional neural network which further finds self correlation from another block. After matching the points, it reconstructs a forgery mask using deconvolutional network but it also sometimes erroneously estimates the authentic but apperently similar regions as forged sections of the image [5].

In another CFMD approach the image is segmented into non-overlapping and uneven blocks adaptively and feature points taken out from every block are matched with each other to identify labeled points.

Feature points are replaced with superpixels as feature blocks and merged with the neighbouring blocks with indistinguishable local color features[6]. Another approach proposed by Yuanman et al. detects forgery through hierarchical feature point matching showing possibility of generating sufficient keypoints for little or untextured areas by lessening the contrast intensity and rescaling the input image and applying a hierarchical matching technique to address the keypoint matching issues over a large number of keypoints [7]. Bi et al. used multi scale feature extraction method wherein a image is divided into the non- overlapping blocks of unalike shapes in various scales and transformed with Scale Invariant Feature Transform (SIFT) [8]to take out feature points from all parts. Multi-scale features are generated and adaptive matching algorithm is used to locate forgeries [9]. Another approach uses SURF[10] key-point detection together with GLCM-based feature descriptors for classification [11]. Al-Quershi et al. proposed a matching technique based on k-means clustering algorithm. k-means clustering caters to the matching step for the blocks. Also the clustering of the feature vectors allowed for accurate matches [12]. This paper addresses the forgery detection involving small smooth regions and solved it by supplementing redundant feature points and feature fusion [13]. Light up shading based forgery area procedure is created here. Getting ready and testing system is used. Distinctive one of a kind and adjusted images are accumulated and their surface and slant features evacuated and the system trained with these features [14]. Threshold based SURF technique is proposed in [15] and the paper claims to have achieved on time and memory savings.

III. PROPOSED APPROACH

Through our approach, one can effectively perform localization of forged regions, as well as classification between forged and authentic images. We have tested our method on both MICC-F220 and MICC-F600 datasets [16].

A. Forged Region Localization

The detection and localisation process is shown in fig. 1. Initially, image is resized into a particular size for the effective distribution of image blocks. The resizing dimensions of the images are determined by the actual size of the image and augmented relatively. Since every Image in MICC-F200 dataset is below 1000 height and 1000 width, then every image is resized into 1024 X 1024 height and width respectively. However, MICC-F600 dataset consists of relatively larger dimension images, though most of the images yield positive detection for image forgery. Alternatively, there were few images which yield negative outcomes even though they are forged. To overcome the sparsity in CASIA 2 dataset, a threshold is taken for resizing the images which can be beneficial for other datasets as well.

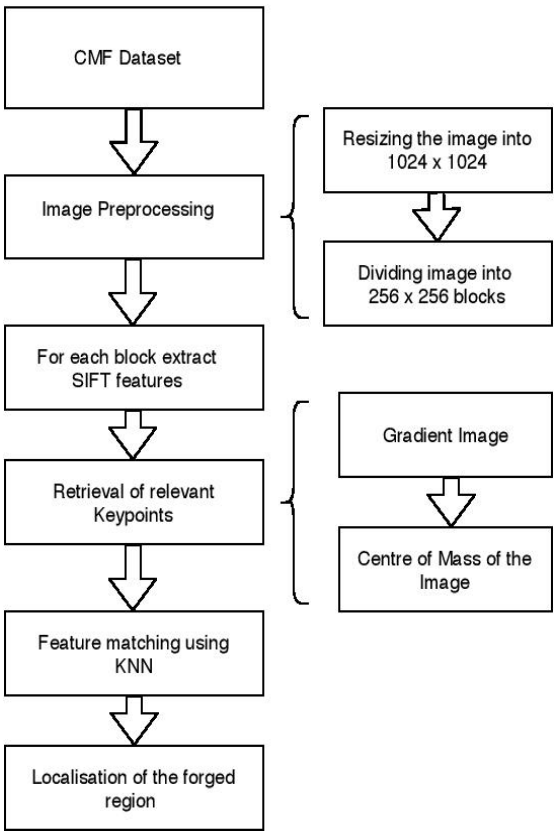
As per our results, we have divided the image into categories to determine the resizing of the images. If the image dimension is both height and width are comparable, we don't resize it. However, if the height and width ratio of the image is higher than 2/3 , then the lower dimension is resized according to the other dimension until it becomes less than 1/4 of the other. Later, that image is divided into equally sized non-overlapping blocks of 256 * 256. SIFT features are extracted for each block which is filtered to select only the relevant approach.

Selecting only the relevant features is achieved through extracting features around the forged region. When the SIFT features are computed for a block, it is passed through a gaussian low pass filter to reduce the noise in that block. After computing the Gaussian low pass filter on that block, the center of mass is calculated. The resultant outcome of performing previous activities provides the center of the image block with a huge probability of localizing forged region. To reduce the plethora of image features extracted through SIFT algorithm the features around the center of mass is taken into consideration.

If the distance between the SIFT keypoint is less than 150 then that keypoint is taken as a relevant feature. Otherwise, that feature is discarded as it doesn't comprehend the forged region, which also reduces the computation in matching features. Finally, obtaining the relevant image features, we compare the features of each block against every other block. In an image, each descriptor is unique if any other block matches with any other block feature than that part are forged.

However, to avoid any pitfalls or false outcomes we have set a 70% threshold of matches between two blocks to accurately mark the forged region.

Fig. 1 Process for localising the forged image



The matching is performed usnig KNN algorithm for faster and accurate results. The forged is marked by creating a 32 X 32 matrix around the matched descriptor to include any missed key points which are forged by SIFT. In order to extend our proposed approach for classification of the images, an image mask is created around the forged region.

B. Classificatıon of Forged and Authentic Images

Once we obtain the image masks, we used them to train our convolutional neural network for accurate classifying between forged and authentic images. Classification is performed after forged image localization to handle the false-positive results which were obtained during image localisation process as shown in fig. 2. Here we have used the output masks obtained from the above-mentioned approach. The output masks are divided into 70% train images, 20% validation images and 10% test images.

We have constructed a two-layer convolutional network followed by a dense network for accurately classifying between forged and authentic images. In between the convolutional network, we have applied dropout layers to reduce the overfitting of the network. Before, transfering images to the CNN, they are reszied into 256 x 256 height and width for keeping each in a common dimension.

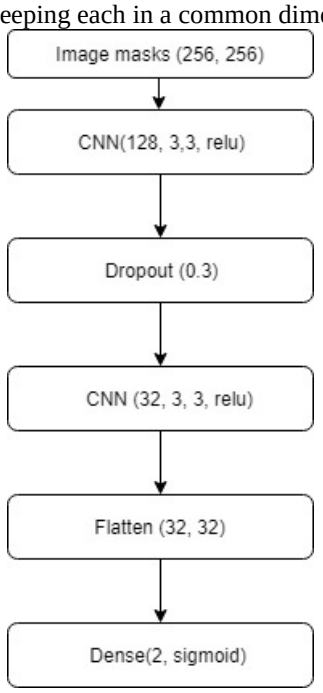


Fig. 2 Process flow for classification between forged and authentic images

IV. RESULTS AND DISCUSSION

We have conducted the experiments on two datasets MICC-F220 and MICC-F600. First, MICC-F220 dataset consists of total 110 forged and 110 authentic images respectively. Second, MICC-F600 consists of 160 tampered images and its corresponding ground truth images. Table I depicts the measure of recall and precision from the experiments, compared with other approaches. Fig. 3. depicts a graphical representation of the results which clearly shows that the technique is better off. Fig. 4. shows the experimental result of how a forged image is localized. of the experiments on images from the datasets used. It is a textured image and still the results are so profound. Fig. 5. shows creation of segmented image mask of the forged region the forged image.

Table- I: Comparison between other approaches for forged image localisation

Approach	Recall	Precision
Al Qureshi	73.48	65.47
Lai et. Al.	36.87	32.35
Ray et. Al	54.09	64.88
Proposed	70.37	95.4

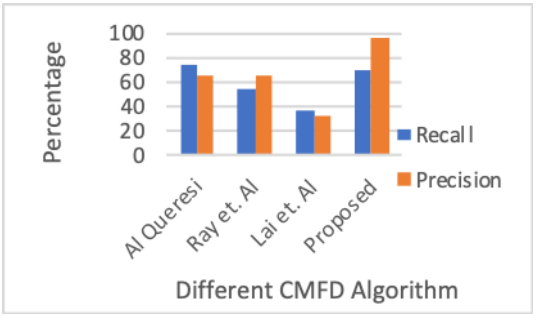


Fig. 3 Graphical comparison between different methods

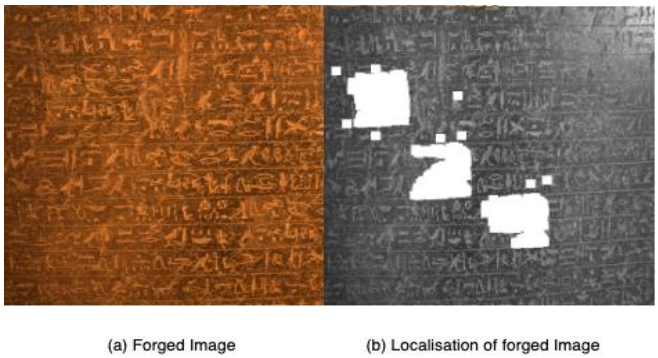


Fig. 4 Some of the experimental results for forged image localization

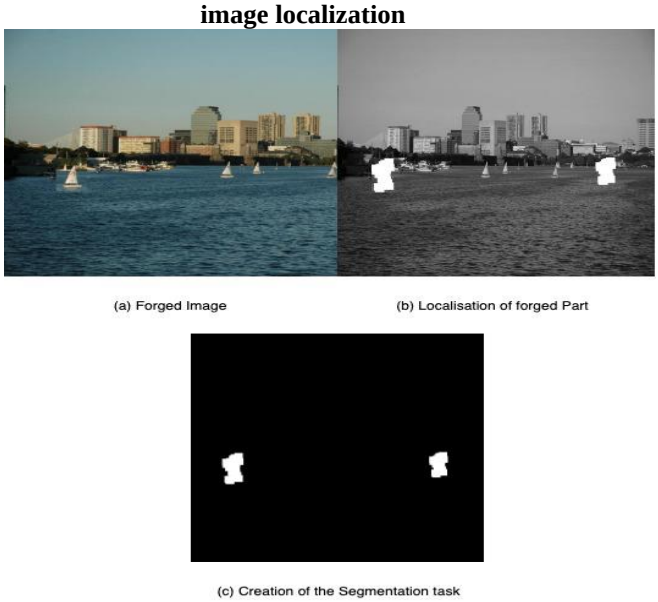


Fig. 5 Example of creating segmented image mask of the forged region.

Table- II: Confusion matrix for localizing the forged image

	Forged	Authentic
Forged	190	80
Authentic	19	251

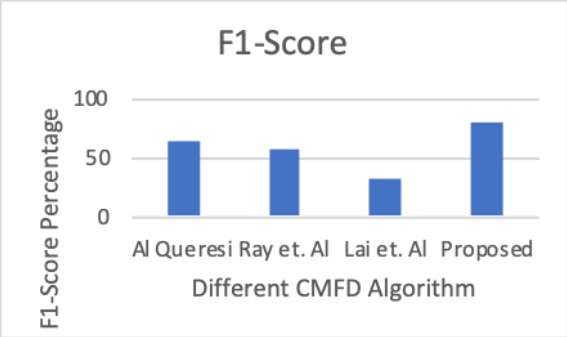


Fig. 6. F-1 score of the proposed approach

V. CONCLUSION

Our paper proposes an efficient approach to overcome some of the problems in the recent era of image forgery detection. Through the proposed approach forged image can effectively be localized which give us a visual representation of the forged regions. In addition to it, the paper provides for a solution for capturing an image mask which is further used to train the convolutional neural network and the tests results of this trained CNN model gives a classification precision of 95.4 % with a comparable recall as shown in the results section.

REFERENCES

1. S. K. Mankar and P. A. A. Gurjar, "Image Forgery Types and Their Detection : A Review," vol. 5, no. 4, pp. 174–178, 2015.
2. T. Das, R. Hasan, M. R. Azam, and J. Uddin, "A Robust Method for Detecting Copy-Move Image Forgery Using Stationary Wavelet Transform and Scale Invariant Feature Transform," *Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2018*, pp. 1–4, 2018.
3. D. Fu, Y. Q. Shi, and W. Su, "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4283 LNCS, pp. 177–187, 2006.
4. M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," *Signal Process. Image Commun.*, vol. 39, pp. 46–74, 2015.
5. Y. Wu, W. Abd-Almageed, and P. Natarajan, "Image copy-move forgery detection via an end-to-end deep neural network," *Proc. - 2018 IEEE Winter Conf. Appl. Comput. Vision, WACV 2018*, vol. 2018-Janua, no. d, pp. 1907–1915, 2018.
6. C. Pun, S. Member, X. Yuan, and X. Bi, "Over - Segmentation and Feature Point Matching," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, pp. 1–12, 2015.
7. Y. Li and J. Zhou, "Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1307–1322, 2019.
8. D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, 2004.
9. X. L. Bi, C. M. Pun, and X. C. Yuan, "Multi-scale feature extraction and adaptive matching for copy-move forgery detection," *Multimed. Tools Appl.*, vol. 77, no. 1, pp. 363–385, 2018.
10. H. Bay, T. Tuytelaars, and L. Van Gool, "SURF: Speeded Up Robust Features BT - Computer Vision – ECCV 2006," 2006, pp. 404–417.
11. S. Teerakanok and T. Uehara, "Copy-move Forgery Detection Using GLCM-Based Rotation-Invariant Feature: A Preliminary Research," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 2, pp. 365–369, 2018.
12. O. M. A. Bee and E. Khoo, "Enhanced block-based copy-move forgery detection using k -means clustering," *Multidimens. Syst. Signal Process.*, 2018.
13. L. Yu, Q. Han, and X. Niu, "Feature point-based copy-move forgery detection: covering the non-textured areas," *Multimed. Tools Appl.*, vol. 75, no. 2, pp. 1159–1176, 2016.
14. R. Sathya, A. K. Sanu, A. Singh, S. Chaurasia, and V. Agrawal, "Detection of Manipulated Images using Convolutional Neural Network," no. 4, pp. 1431–1438, 2019.
15. P. Srivastava, M. Kumar, V. Deep, and P. Sharma, "A Technique to Detect Copy-Move Forgery using Enhanced SURF," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6S, pp. 676–680, 2019.
16. 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 Trans. Inf. Forensics Secur.*, vol. 6, no. 3 PART 2, pp. 1099–1110, 2011.

AUTHORS PROFILE

Ritu Agarwal received her M.Tech degree in Information Security from Ambedkar Institute Of Advanced Communication Technologies And Research (formerly Ambedkar Institute of technology), Delhi. She is currently working as an Assistant Professor in the Department of Information Technology at Delhi Technological University,(formerly Delhi College of Engineering), Delhi India since 2010, and pursuing her Ph.D. in Information Technology. Her research interests include Information Security, Data Recovery, Digital Forensics, Cyber Forensics, data structures, analysis and design of algorithms, pattern mining.

Om Prakash Verma received his B.E. degree in electronics and communication engineering from the Malaviya National Institute of Technology, Jaipur, India, M.Tech. degree in communication and radar engineering from the Indian Institute of Technology, Delhi, New Delhi, India, and the Ph.D. degree in the area of applications of soft and evolutionary computing in image processing from the University of Delhi, New Delhi, India.

From 1992 to 1998, worked as Assistant Professor with Department of Electronics and Communication Engineering, Malaviya National Institute of Technology, Jaipur, India. Later joined the Department of Electronics and Communication Engineering, Delhi Technological University (formerly Delhi College of Engineering), New Delhi, India, as an Associate Professor in 1998, and is currently Professor at Delhi Technological University. His current research interests include applied soft computing, nature inspired algorithms, swarm intelligence, evolutionary computing, and image processing.