

Tampering Detection using Resampling Features and Convolution Neural Networks

Manjunatha. S, *¹, Malini M Patil.²

¹ Department of information Science & Engineering., Global Academy of Technology, Bengaluru, 560 098, India

²Department of Information Science & Engineering, J S S Academy of Technical Education

Bengaluru,560 060, India

manjunaths.dvg@gmail.com¹, drmalinimpatil@gmail.com²

Manjunatha S*: Phone: +91-9886033445

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: The increased usage of image editing tools has resulted in the ease of manipulating multimedia data such as images. These manipulations affect the truthfulness and legitimacy of images, resulting in misinterpretation and may affect social stability. The image forensic technique has been utilized for detecting whether an image is tampered with using certain attacks such as splicing, copy-move, etc. This paper presents an efficient tampering detection method using resampling features (RSF) and Convolution neural network (CNN). In RSF-CNN, during preprocessing the image is divided into homogenous patches. Then, within each patch resampling features are extracted by exploiting affine transformation and Laplacian operator. Then, features extracted are aggregated for constructing descriptors using Convolution neural network. Extensive analysis is carried out for evaluating tampering detection and tampered region segmentation accuracies of proposed RSF-CNN based tampering detection methodologies considering various distortions and post-processing attacks such as joint photographic expert group (JPEG) compression, scaling, rotations, noise additions, and multiple manipulations. From the result achieved it can be seen the RSF-CNN based tampering detection model achieves much better accuracies than existing tampering detection methodologies.

Keywords: Deep learning, Convolution neural network, Image tampering detection, Image transformation, Resampling feature extraction.

1. Introduction

With increased exposure to the internet because of the cheap availability of smartphones and bandwidth has led to increased usage and sharing of multimedia data on the online environment such as WhatsApp, Facebook, Instagram, Youtube, etc. This growth led to the emergence of various digital image editing software's leading to trust issues of photography being shared. Building well-crafted tampering is well within the reach of end-users especially with the introduction of artificial intelligence (AI) enabled multimedia data editing software tool. Some of the well-known software editing tools are FaceApp [1]- which is used for editing the age of the person and facial expressions, Adobe Sensei [2]- which is used to enhance or beautify the faces, Deep Photo Style Transfer [3]- which are used for changing the visual appearance of an image such as time-of-day hallucination, weather, etc. Adobe Sky Replace [4]- which is used for matching lighting, replacing skies, etc. A number of these editing techniques are readily available in smartphones and devices [5]. As humans fail to distinguish between genuine and fake images [6], thus it is important to develop an automating tampering detection scheme with high accuracies is utmost importance in a wide range of applications and services.

The discovery of multimedia content tampering has become extremely challenging and difficult as tampered images look very much identical with respect to the authenticated image. With the growth of cutting-edge multimedia editing software, a picture can tamper from multiple points of view. These tampering can be classified into the following types such as content changing and content preserving [7]. The primary tampering methodologies such as object removal, splicing, copy-clone, etc. randomly alter the complete image and also semantically alters the meaningful representation of the image [7]. On the other side, the secondary tampering methodologies such as contrast enhancement, blurring, compression, etc. are generally done during post-processing operations and are less problematic as they do not change the semantic representation of an image. Thus, this paper focuses on addressing content changing problems. The content-changing tampering will lead in give misappropriate and deceptive information. The increased use of social media platforms for exchanging multimedia content has resulted in an increased number of tampering; thus it is very much important to identify the tampered image for preventing users from viewing deceptive information. As of late, content-changing tampering detection using image or video has attained wide-attention across the research community considering different surety and surveillance applications.

This paper presented new methodologies for detecting tampering and localization of tampered segment at the pixel level for content changing manipulation.

Recently, extensive researches have been carried out for classifying image tampering, that is, to detect whether an image is manipulated or not [8], [9], [10]. Among the very limited research has focused on localizing tampered segments at pixel level [11], [12]. In [13], [14] addressed tampering location detection by classifying whether a patch is tampered with or not. Identifying tampering location is a challenging and difficult job as tampered images don't provide any visual piece of information/evidence, as displayed in Fig. 1. In Fig. 1, copy-clone tampering is shown where a particular segment of an image is copied and pasted onto a different region within the same image resulting in two similar objects, one is a tampered object and the other is an original object. The splicing tampering is shown in Fig. 2, where an object from one image is removed and placed onto another image. The majority of existing tampering detection methodologies use the frequency domain statistical feature or characteristic of multimedia content [15], [16]. In [16], [17] use artifacts measurement from multiple JPEG compressions for detecting tampered images, though the model only works for JPEG formats. In [18] for improving resampling detection performance added noise into the JPEG compressed image. Recently, deep learning has attained good performance in computer vision such as segmentation, scene classification, and object detection [19], [20], [21].

In recent time, number of deep learning-based tampering detection [34], [35], [36] such as convolutional neural networks (CNN) [22],[23], [37] and stacked auto-encoders (SAE) [24] have been presented. In a media crime scene investigation, the majority of state-of-art tampering detection methodologies have focused on detecting certain types of tampering only such as splicing [25] and copy-clone [26]. Thus, some methodologies might work for one kind of tampering and perform badly for other types of tampering. Besides, it appears to be impracticable to know in advance the type of tampering. This work presents an improved tampering detection methodologies by extending the work presented in [11] for designing a framework to detect different kinds of image tampering.

In contrast with semantic object segmentation where different semantic segments are extracted, this work focuses only on identifying the tampered segments which makes it, even more, challenging task. Recently, CNN based semantic segmentation methodologies [20], [27] have attained attention. In [27], used fully connected CNN for analyzing region shape and object content by extracting feature sets at different levels in a hierarchical manner. The CNN based framework works very well in the area of object detection [19] and segmentation [20], [27] in learning and a better understanding of the content of different segments. Unlike object segmentation, tampered segments could be copied objects from different regions of an image or could be removed objects. A good tampered image will have good similarities among authenticated and fake images [23]. Even though the convolution neural network produces spatial maps for different segments of multimedia content, they achieve very poor performance in generalizing different artifacts induced by different tampering methodologies. As a result, the tampering region segmentation using a standard convolution neural network may not produce a good result.

In [11], carried out a comparative analysis of various existing tampering region segmentation methodologies [20], [27] and showed they do not perform well for object removal and copy-move tampering. Image forgeries create certain artifacts such as compression, resampling, etc. which are can be better learned using resampling features [13], [28]. Due to interpolation resampling introduces periodic correlation between the pixels. The CNN shows good translational invariance to produce spatial maps across different segments of multimedia content, and certain artifacts are well-learned using resampling feature sets [38]; which can be utilized to locate tampered segments. Thus, this paper presents an efficient image tampering detection scheme using resampling features and a convolution neural network. Here the resampling features are extracted by employing affine transformations and the Laplacian operator. Then, descriptors are constructed using CNN for predicting whether the image is tampered with or not.

The contribution of research work.

- This paper presented an efficient tampering detection scheme exploiting resampling features and convolutional neural networks.
- The RSF-CNN based tampering detection scheme can detect multiple tampering within the image more efficiently when compared with the existing tampering detection scheme.
- The RSF-CNN based tampering detection scheme achieves very good tampering segmentation outcomes when compared with the existing tampering detection scheme.
- The RSF-CNN based tampering detection method achieves better recall, precision, and F1-score performance than existing tampering detection methodologies.

The manuscript is arranged as follows. Section 1, discusses tampering detection issues and challenges, the benefit of using resampling features and convolution neural network, and the significance of work is discussed. In section 2, the proposed tampering detection methodologies using resampling features and convolution neural

network. In section 3, the tampering detection accuracies and segmentation outcome achieved by proposed RSF-CNN based tampering detection methodologies over existing tampering detection methodologies. In section 4, the paper is concluded with research significance and the future direction of work is also discussed.

2. Tampering Detection using Resampling Feature and Convolution Neural Networks

This section presents the image tampering methodologies using resampling features and convolution neural networks. First, present preprocessing and resampling feature extraction for tampering detection. Second, the extracted features are trained using a convolution neural network for detecting whether the image has tampered or not.

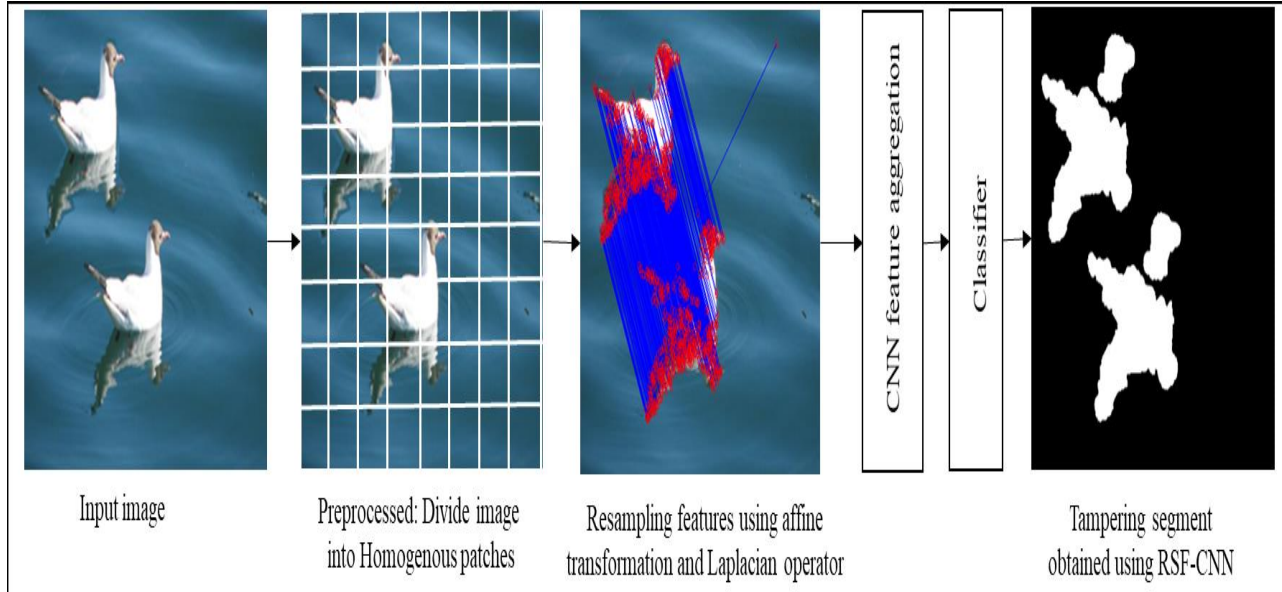


Fig. 1. Proposed RSF-CNN based tampering detection methodologies.

2.1 Preprocessing and resampling feature detection and extraction:

In general, the images are tampered with using the following operations such as object removal, splicing, and copy-move, etc. This tampering affects the statistical feature alongside the edges of the forged segments. In [29], the resampling detection method is presented using affine transformation and Laplacian operator for extracting the resampling features for respective patches. This work uses a similar methodology for the extraction of resampling features in a given image. First, the image is segmented into a non-overlapping patch size of 64 (i.e., 8×8). When considering an image with a size of 512×512 , then each patch dimension size will be 64 . Further, for producing magnitude of linear projected error for different patches Laplacian operator is used [13]. For accumulating errors with respect to a different angle of projection this work uses affine transformation because there exist periodic correlations among resampling signals. At last, Fast Fourier Transform (FFT) is applied for identifying the resampling features periodic characteristic of the signals. Generally, the resample feature sets have the capability of identifying different resampling nature such as rotation, up- or down-sampling, and JPEG thresholding, etc.

For bringing good tradeoffs between increasing accuracy and reducing computation complexity here the image is resized to 512×512 which may induce certain artifacts such as up- or down-sampling, image quality variations, etc. In [13] showed that the resampling feature can be utilized for classifying the aforementioned artifacts. Further, resampling feature sets are used for classifying patches. However, in this work, it is used for localizing at the pixel level. For obtaining a higher number of features it is important to bring good tradeoffs in choosing the patch size. This is because resampling signal can be easily established in larger patch size as it will have a higher amount of repeated features; however, identifying small tampered segments will be difficult for localizing it. The existing resampling based tampering detection methodologies extracted resampling features considering block size of 32×32 . However, in this work patch size is set to 64 for obtaining more useful information. The main factor of using resampling feature within the patches is to establish the nature of local artifacts because of different tampering.

The outcome of CNN mainly depends on the organization of the patches. It can either be ordered in vertical or horizontal directions; however, it fails to obtain relevant local feature information. This is because, if we are arranging the patches in a vertical direction, then the patch sets of different neighbors horizontally will be disconnected by a complete column of patches. Thus, takes a lot of time and CNN fails to bring good correlation among these patches. Similarly, if we traverse through horizontal direction over the rows will result in the same problem. For preserving special features of different patches, this work uses a space-filling curve[30] which is widely utilized for reducing multi-dimensional problems to one-dimensional problems [31], [32], and [33].

2.2 Feature aggregations using CNN for tampering detection:

In the feature extraction phase, we obtain a large number of features, these features are aggregated for constructing descriptor in classifying whether an image is a tamper or not and identifying and segment the forged region. Here different kind of aggregator function is considered such as minimum, maximum, mean, and mean of squares which are described below [39]. The minimum aggregation function is described below

$$G_{\downarrow} = \min_{j=1, \dots, O_q} G_j \tag{1}$$

The maximum aggregation function is described below

$$G_{\uparrow} = \max_{j=1, \dots, O_q} G_j \tag{2}$$

The mean aggregation function is described below

$$G_{\rightarrow} = \frac{1}{O_q} \sum_{j=1}^{O_q} G_j \tag{3}$$

The mean of square aggregation function is described below

$$G_{\leftarrow} = \frac{1}{O_q} \sum_{j=1}^{O_q} G_j^2 \tag{4}$$

where O_q depicts the patch size considered for extracting features, $G_j = [G_{j,1}, \dots, G_{j,d}]$ represents the d -component feature extracted within the O_q path. Selection of type of averaging/pooling function depends on the type of image and type of problems to be addressed. When tampering is spread across the entire image, in such case averaging function works reasonably well, on the other side, the maximum and minimum function performs better correlative feature is focused within localized segments. Nonetheless, in this work, we use a different kind of pooling function for experiments. Finally, the spatial dependencies are eliminated after aggregating features.

An important thing to be noted here is the selection of pooling functions impacts in what way the feature information is back-propagated from the output layer for updating parameter of the feature extraction operation. For providing more detailed modeling, let θ be a generic parameter of convolution neural network, M depicts the loss function CNN architecture, and $G_{agr,d}$ represent the aggregated features. Then, the gradient of M considering generic parameter θ reads

$$\frac{\partial M}{\partial \theta} = \sum_{d=1}^D \frac{\partial M}{\partial G_{agr,d}} \frac{\partial G_{agr,d}}{\partial \theta} \tag{5}$$

with

$$\frac{\partial G_{agr,d}}{\partial \theta} = \begin{cases} \frac{\partial G_{j,d}}{\partial \theta} \cdot \mu_{j,j_{\uparrow}(d)} & \text{max pooling} \\ \frac{\partial G_{j,d}}{\partial \theta} \cdot \mu_{j,j_{\downarrow}(d)} & \text{min pooling} \\ \frac{1}{O_q} \sum_{j=1}^{O_q} \frac{\partial G_{j,d}}{\partial \theta} & \text{average pooling} \\ \frac{1}{O_q} \sum_{j=1}^{O_q} 2G_{j,d} \frac{\partial G_{j,d}}{\partial \theta} & \text{avg.sqr pooling} \end{cases} \quad (6)$$

From Eq. (5) and (6) it can be seen, $\mu_{j,j_{\uparrow}(d)}$ will be equal to $\mu_{j,j_{\downarrow}(d)}$ when $j = j_{\uparrow}(d) = j_{\downarrow}(d)$ and if the condition fails it will be $\mu_{j,j_{\uparrow}(d)} > \mu_{j,j_{\downarrow}(d)}$ while $j_{\uparrow}(d)$ describes a feature vector with largest component and $j_{\downarrow}(d)$ describes a feature vector with smallest component. As a result, using minimum or maximum pooling function, only some active patches play a major factor in the gradient, and optimize the CNN learning model. On the other side using the mean and mean square pooling function the entire patches play a role in the gradient. Nonetheless, if different pooling functions are utilized for training at the same instance, in such case the gradient is optimized as a weighted sum of individual terms.

2.3 Decision:

After aggregating the feature from different patches of an image of a descriptor d , this is done using few fully-connected layers similar to deep networks. For bringing good tradeoffs between achieving higher accuracy with reduced computation complexities just two-layer is used in this work.

2.4 Training of CNN:

Here the work focuses on the post-training functions, the resampling feature-based CNN (RSF-CNN) framework is very similar to standard methodologies based on patch-based feature extraction, aggregation, and classification. However, the major difference is that the RSF-CNN model can be trained end-to-end. Thus, there is no need to train the classification model with features extracted using the fixed network. Rather, the model can be trained as a whole framework on the complete image to classify whether the image has tampered or not. The loss function back-propagates within the net up to distinct patch sets, which aids feature extractor to learn which feature is more correlated for the final decision, and the makes CNN model to work jointly with resampling feature extractor in an adaptive manner. The proposed tampering detection method using resampling features and CNN attain superior performance when compared with the existing tampering detection method which is experimentally shown in the below section.

3. Result and Discussion

This section presents a performance evaluation of the proposed RSF-CNN based tampering detection method over the existing tampering detection method. The RSF-CNN based tampering detection method is implemented using Python, C++, and Matlab library. The experiment is conducted on MICC-600, MICC-Multi, and D0 dataset. The dataset description used for experiment analysis is shown in Table I. The performance of RSF-CNN and the existing tampering detection method are evaluated in terms of the following metrics such as True positive rate (TPR) (i.e., recall), F1 score, and False Positive rate (FPR). To verify the performance of the proposed RSF-CNN based image forensics, the experimental results are compared to existing tampering detection methodologies [40], and [41] to perform the forgeries, including copying and translations, scaling, rotation, and compression.

Table I: Dataset considered for experiment analysis

Dataset	Number of images	JPEG compression	Scaling and rotation
MICC	600	No	Yes
D0	50	yes	Yes

3.1 Performance evaluation on MICC dataset

The experiment is conducted using the MICC dataset. MICC-600 consists of 600 images: 300 images have tampered images and 300 are originals. The size of the forged patch covers, on average, 1.2% of the whole image. The outcome achieved using the proposed RSF-CNN based tampering detection method is shown in Figure 2. Further, the accuracy performance of the proposed RSF-CNN based tampering detection method over the existing tampering detection method is carried is shown in Table II. Further, from Figure. 3 it can be seen the proposed RSF-CNN model achieves a better segmentation outcome of the tampered region. From the result achieved it can be seen the proposed RSF-CNN based tampering detection method achieves a much superior outcome than the existing tampering detection method in terms of Recall/TPR, FPR, and F1-Score for the MICC dataset. Thus, the proposed RSF-CNN based tampering detection method is robust in detecting forged segments considering rotation and scaling.

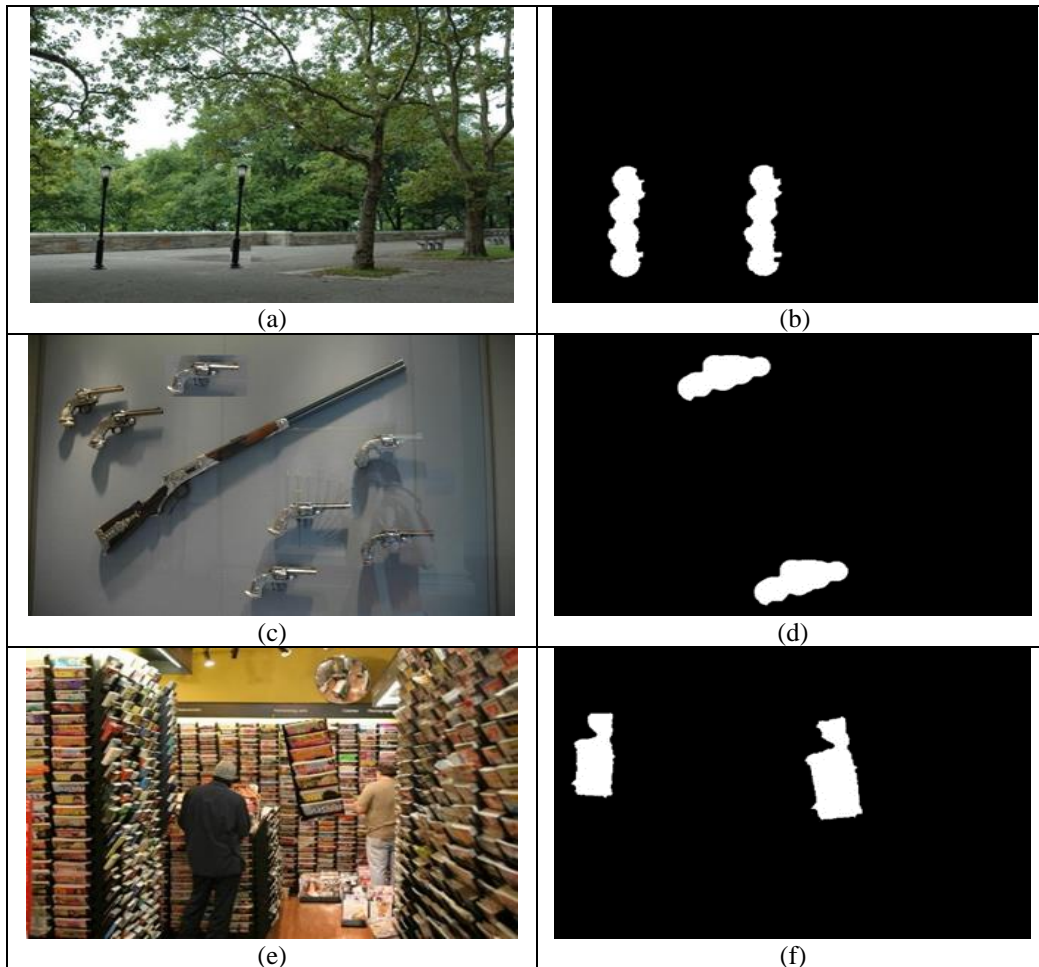


Fig. 2. The output of the proposed tampering detection method.



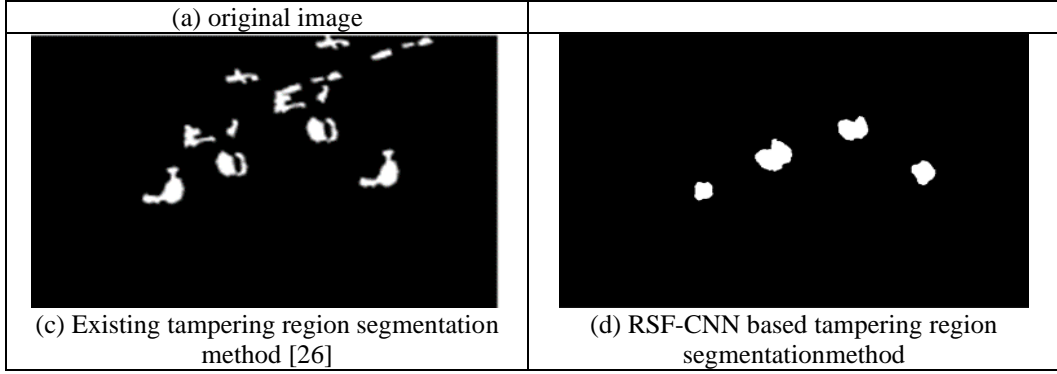


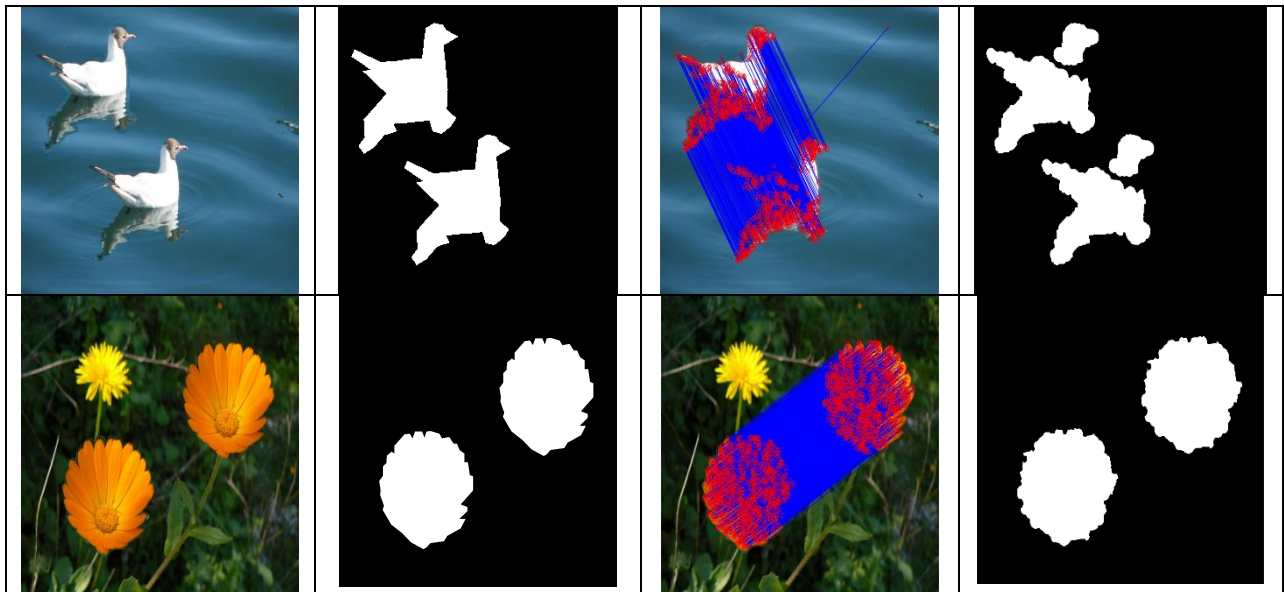
Fig. 3. Comparative analysis of proposed RSF-CNN based tampering detection method over existing tampering detection methodology.

Table II: Comparative analysis of proposed RSF-CNN based tampering detection method over existing tampering detection method for MICC dataset

	Recall/TPR	FPR	F1-Score
Raju et al., 2018 [40]	89.14	-	92.6
RSF-CNN	97.5	1.4	97.7

3.2 Performance evaluation on D0 dataset

An experiment is conducted using the D0 dataset to detect whether an image has tampered or not using the proposed RSF-CNN based tampering detection method using resampling features and CNNs. The dataset includes the tampered images in which every copy-pasted area is transformed according to the following transformations: rotation in the range of $[-25^\circ, 25^\circ]$ with step 5° , rotation in the range of $[0^\circ, 360^\circ]$ with a step of 30° , rotation in the range of $[-5^\circ, 5^\circ]$ with a step of 1° , scaling in the range of $[0.25, 2]$ with step 0.25 , and scaling in the range of $[0.75, 1.25]$ with step 0.05 . The outcome achieved using the proposed RSF-CNN based tampering detection method is shown in Figure 4. Further, the accuracy performance of the proposed RSF-CNN based tampering detection method over the existing tampering detection method is carried is shown in Table III. From the result achieved it can be seen the proposed resampling feature-based tampering detection method achieves a much superior outcome than the existing tampering detection method in terms of precision, recall, and FPR, and F1-score for the D0 dataset. Thus, the proposed RSF-CNN based tampering detection method is robust in detecting forged segments considering rotation and scaling. To estimate the robustness of our approach against false positive detection, we used an untampered dataset (D3 dataset) to verify our approach.



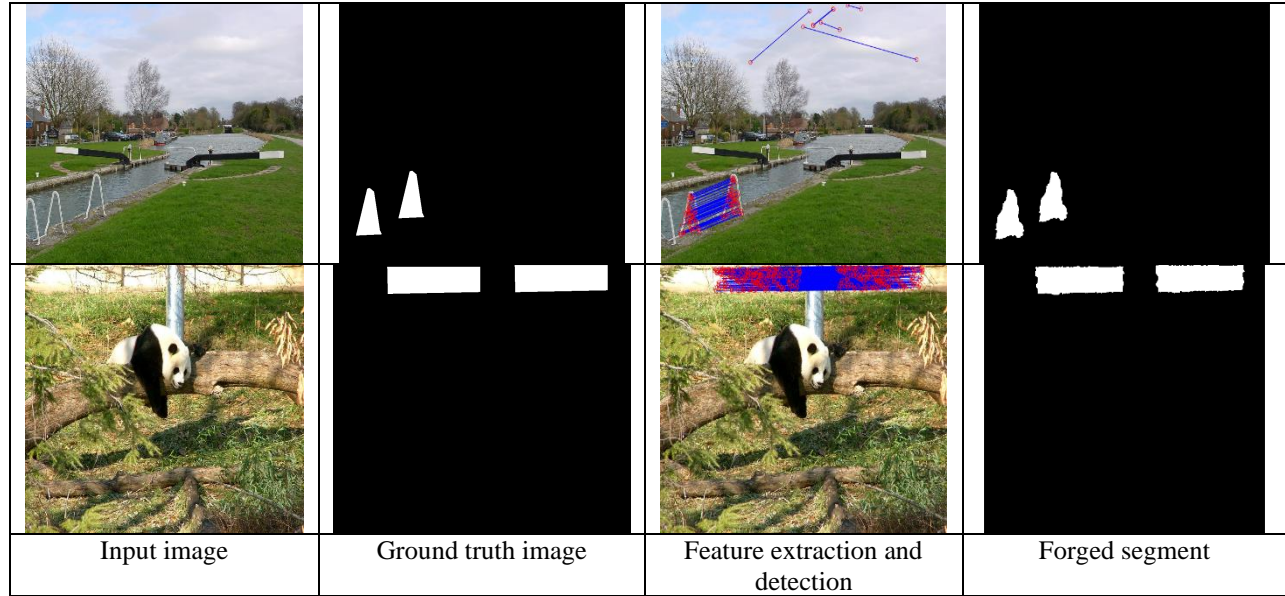


Figure 3. a) input image, b) corresponding groundtruth image, final feature extracted, and d) the transformed forged segment image using proposed tampering detection using resampling features and CNN.

Table III: Comparative analysis of proposed RSF-CNN based tampering detection method over existing tampering detection method for D0 dataset

Model	Recall	Precision	FPR	F1
Huang et al. 2019	84.88	92.81	3.39	88.67
RSF-CNN	98.08	98.84	1.68	99.28

4. Conclusion

This paper present a tampering detection method using resampling features (RSF) and convolution neural network (CNN). The RSF-CNN based tampering detection methodologies can effectively classify forged and non-forged segments and can semantically segment the forged region. The RSF-CNN model can retain spatial features by using resampling features among different patches and establish a correlation between tampered and non-tampered patches. Then, these resampling features are aggregated for eliminating spatial dependencies, and a descriptor is built for the whole image. An experiment is conducted on standard MICC and D0 datasets which includes different copy-clone, scaling, rotation, and compression. From the results attained it can be seen the RSF-CNN based tampering detection model achieves a much superior True positive rate, F1 score, and False Positive rate when compared with the existing tampering detection model.

Despite very good results attained, the model can be further improved by improving the quality of feature extraction with a reduced outlier. Then, develop a new CNN framework for mitigating the effects of noiseaffecting the spatial relationship. Thus, future work would consider the aforementioned problems in developing improved tampering detection methodologies. Further, performance evaluation will be considered more diverse tampering attack datasets.

Reference

1. FaceApp, <https://www.faceapp.com/>, visited 11 Sept. 2020.
2. Adobe Sensei, <http://www.adobe.com/sensei.html>, visited 11 Sep. 2020.
3. F. Luan, S. Paris, E. Shechtman, K. Bala, Deep photo style transfer, arXiv preprint arXiv:1703.07511, 2017.
4. Adobe Sky Replace, <https://research.adobe.com/sky-replace/>, visited 11 Sept. 2020.
5. Xiaomi Selfie Beautification, <http://www.businessinsider.com/xiaomi-selfie-beautification-2015-2?IR=T>, visited 11 Apr. 2020.
6. V. Schetinger, M. Oliveira, R. DaSilva, T. Carvalho, Humans are easily fooled by digital images, arXiv preprint arXiv:1509.05301, 2015, <https://arxiv.org/abs/1509.05301>, 2015.

7. R. M. Joseph and A. Chithra. Literature survey on image manipulation detection. *International Research Journal of Engineering and Technology (IRJET)*, 2(04), 2015.
8. M. Jaber, G. Bebis, M. Hussain, and G. Muhammad. Accurate and robust localization of duplicated region in copy-move image forgery. *Machine vision and applications*, 25(2):451–475, 2014.
9. H. Li, W. Luo, X. Qiu, and J. Huang. Image forgery localization via integrating tampering possibility maps. *IEEE Transactions on Information Forensics and Security*, 12(5):1240–1252, 2017.
10. C.-M. Pun, X.-C. Yuan, and X.-L. Bi. Image forgery detection using adaptive over-segmentation and feature point matching. *IEEE Transactions on Information Forensics and Security*, 10(8):1705–1716, 2015.
11. J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. Manjunath. Exploiting spatial structure for localizing manipulated image regions. In *ICCV*, 2017.
12. L. Bondi, S. Lameri, D. G`uera, P. Bestagini, E. J. Delp, and S. Tubaro. Tampering detection and localization through clustering of camera-based CNN features. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 1855–1864, 2017.
13. J. Bunk, J. H. Bappy, T. M. Mohammed, L. Nataraj, A. Flenner, B. Manjunath, S. Chandrasekaran, A. K. Roy-Chowdhury, and L. Peterson. Detection and localization of image forgeries using resampling features and deep learning. In *Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017 IEEE Conference on, pages 1881–1889, 2017.
14. Y. Liu, Q. Guan, X. Zhao, and Y. Cao. Image forgery localization based on multi-scale convolutional neural networks. *arXiv preprint arXiv:1706.07842*, 2017.
15. B. Mahdian and S. Saic. Detection of copy-move forgery using a method based on blur moment invariants. *Forensic science international*, 171(2):180–189, 2007.
16. W. Wang, J. Dong, and T. Tan. Exploring DCT coefficient quantization effects for local tampering detection. *IEEE Transactions on Information Forensics and Security*, 9(10):1653–1666, 2014.
17. I.-C. Chang, J. C. Yu, and C.-C. Chang. A forgery detection algorithm for exemplar-based inpainting images using multi-region relation. *Image and Vision Computing*, 31(1):57–71, 2013.
18. L. Nataraj, A. Sarkar, and B. S. Manjunath. Improving re-sampling detection by adding noise. In *Media Forensics and Security II*, volume 7541, page 75410I. *International Society for Optics and Photonics*, 2010.
19. R. Girshick. Fast r-CNN. In *IEEE International Conference on Computer Vision*, 2015.
20. J. Long, E. Shelhamer, and T. Darrell. Fully convolutional networks for semantic segmentation. In *IEEE Conference on Computer Vision and Pattern Recognition*, 2015.
21. B. Zhou, A. Lapedriza, J. Xiao, A. Torralba, and A. Oliva. Learning deep features for scene recognition using a places database. In *Advances in neural information processing systems*, 2014.
22. B. Bayar and M. C. Stamm. A deep learning approach to universal image manipulation detection using a new convolutional layer. In *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, pages 5–10, 2016.
23. Y. Rao and J. Ni. A deep learning approach to the detection of splicing and copy-move forgeries in images. In *IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016.
24. Y. Zhang, L. L. Win, J. Goh, and V. L. Thing. Image region forgery detection: A deep learning approach. In *Proceedings of the Singapore Cyber-Security Conference (SG-CRC)*, 2016.
25. V. Manu and B. Mehtre. Visual artifacts based image splicing detection in uncompressed images. In *IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS)*, 2015.
26. J. Li, X. Li, B. Yang, and X. Sun. Segmentation-based image copy-move forgery detection scheme. *IEEE Transactions on Information Forensics and Security*, 10(3):507–518, 2015.
27. V. Badrinarayanan, A. Kendall, and R. Cipolla. Segnet: A deep convolutional encoder-decoder architecture for scene segmentation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2017.
28. S.-J. Ryu and H.-K. Lee. Estimation of linear transformation by analyzing the periodicity of interpolation. *Pattern Recognition Letters*, 36:89–99, 2014.
29. B. Mahdian and S. Saic. Blind authentication using periodic properties of interpolation. *Information Forensics and Security, IEEE Transactions on*, 3(3):529–538, Sept. 2008.
30. D. Voorhies. Space-filling curves and pace-filling curves and a measure of coherence. *Graphics Gems II*, page 26, 1991.
31. B. Moon, H. V. Jagadish, C. Faloutsos, and J. H. Saltz. Analysis of the clustering properties of the Hilbert space-filling curve. *IEEE Transactions on Knowledge and Data Engineering*, 13(1):124–141, Jan 2001.
32. T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, B. Manjunath, S. Chandrasekaran, A. K. Roy-Chowdhury, and L. Peterson. Boosting image forgery detection using resampling detection and copy-move analysis. 2018.

33. B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," 2017 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), New Orleans, LA, pp. 2152-2156, DOI: 10.1109/ICASSP.2017.7952537, 2017.
34. L. Jiao and J. Zhao, "A Survey on the New Generation of Deep Learning in Image Processing," in IEEE Access, vol. 7, pp. 172231-172263, DOI: 10.1109/ACCESS.2019.2956508, 2019.
35. Z. J. Barad and M. M. Goswami, "Image Forgery Detection using Deep Learning: A Survey," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, pp. 571-576, DOI: 10.1109/ICACCS48705.2020.9074408, 2020.
36. Kuznetsov, "Digital image forgery detection using deep learning approach" Journal of Physics: Conference Series, IOP Publishing, vol. 1368, pp. 1742-6596, DOI: 10.1088/1742-6596/1368/3/032028, 2019.
37. Huang, R., Fang, F., Nguyen, H.H., Yamagishi, J., & Echizen, I. A Method for Identifying Origin of Digital Images Using a Convolution Neural Network. ArXiv, abs/1911.00655, 2019.
38. Flenner, Arjuna & Peterson, Lawrence & Bunk, Jason & Mohammed, Tajuddin Manhar & Nataraj, Lakshmanan & Manjunath, B. Resampling Forgery Detection Using Deep Learning and A-Contrario Analysis. Electronic Imaging. 2018. 10.2352/ISSN.2470-1173.2018.07.MWSF-212, 2018.
39. Marra, Francesco & Gragnaniello, Diego & Verdoliva, Luisa & Poggi, Giovanni. A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection, 2019.
40. Raju, Priya & S. Nair, Madhu. Copy-move forgery detection using binary discriminant features. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2018.11.004, 2018.
41. Huang, H., Ciou, A. Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. J Image Video Proc. 2019, 68 (2019). <https://doi.org/10.1186/s13640-019-0469-9>, 2019.