Indonesian Journal of Electrical Engineering and Computer Science
Vol. 25, No. 1, January 2022, pp. 183~190
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v25.i1.pp183-190

Efficient resampling features and convolution neural network model for image forgery detection

Manjunatha S[1,2], Malini M. Patil[3]
[1]Department of Information Science and Engineering, Global Academy of Technology, Bengaluru, India
[2]Department of CSE, J.S.S Academy of Technical Education Bengaluru, Bengaluru, India
[3]Department of Information Science and Engineering, J.S.S Academy of Technical Education, Bengaluru, India

Article Info

Article history:

Received Feb 4, 2021
Revised Oct 31, 2021
Accepted Dec 1, 2021

Keywords:

Convolution neural network
Deep learning
Hybrid attack
Image tampering detection
Resampling feature

ABSTRACT

The extended utilization of picture-enhancing or manipulating tools has led to ease of manipulating multimedia data which includes digital images. These manipulations will disturb the truthfulness and lawfulness of images, resulting in misapprehension, and might disturb social security. The image forensic approach has been employed for detecting whether or not an image has been manipulated with the usage of positive attacks which includes splicing, and copy-move. This paper provides a competent tampering detection technique using resampling features and convolution neural network (CNN). In this model range spatial filtering (RSF)-CNN, throughout preprocessing the image is divided into consistent patches. Then, within every patch, the resampling features are extracted by utilizing affine transformation and the Laplacian operator. Then, the extracted features are accumulated for creating descriptors by using CNN. A wide-ranging analysis is performed for assessing tampering detection and tampered region segmentation accuracies of proposed RSF-CNN based tampering detection procedures considering various falsifications and post-processing attacks which include joint photographic expert group (JPEG) compression, scaling, rotations, noise additions, and more than one manipulation. From the achieved results, it can be visible the RSF-CNN primarily based tampering detection with adequately higher accurateness than existing tampering detection methodologies.

Corresponding Author:

Manjunatha S
Department of Information Science and Engineering, Global Academy of Technology
Bengaluru, India
Email: manju.dvg2020@gmail.com

1. INTRODUCTION

The emergence of social networks in our daily life spurs the advent of various digital image editing tools which leads to belief issues of multimedia content being circulated. Designing high-quality tampering employing a machine learning model that is visually undetectable through the human eye [1], [2] is well within reach of the user through the following tool such as FaceApp [3], Adobe Sensiei [4], DeepPhoto editor [5], and Adobe sky Replace [6]. Thus, classifying an image as tampered with or not is becoming an extremely difficult task. In general, tampering is classified into content preserving and changing [7]. The copy-clone, splicing, and object exclusion are widely used primary attacks, and blurring, compression, and contrast adjustment are commonly used secondary attacks. However, the primary attack will result in a semantical illustration of an image. Thus, this work focuses on detecting the primary attack.

Recently, several methods have been presented for detecting primary tampering attacks [8]-[10]. However, these methods have focused on detecting whether an image is tampered or not and failed to localize tampered region within a tampered image [11], [12]. In [13], [14] able to localize the patches that are tampered with through the employment of frequency domain [15], [16]. Sudiatmika *et al*. [17] used noisy information [18] of compressed image for establishing whether the image has tampered or not. In recent times deep learning techniques have achieved a very good result in computer vision applications [19]-[21] including image tampering detection and classification [22], [23]. The autoencoder [24] and convolution neural network (CNN) [22], [23] have been widely used to detect primary attacks such as splicing [24], [25] and copy-move [26]. However, these model fails to provide good accuracy when image undergoes a hybrid transformation as they are designed to detect either splicing or copy-move. Further, the traditional fully-connected CNN-based framework [27] fails to generalize different noise induced through different tampering detection methods; thus, poor tampering region localization outcome is achieved.

In addressing such issues in this work presented an improved tampering detection model employing improved preprocessing, feature aggregation, and CNN architecture [11]. Bunk *et al*. [11] showed, image tampering induces noise because of periodic interpolation among adjacent pixels which can be understood through resampling features [13], [28]. Here affine transformation and Laplacian function is used for extracting resampling features and descriptor is built through CNN. The significance of range spatial filtering (RSF)-tamper detection (TD) is described next. The paper presented a CNN-based tampering detection method by learning Resampling Features. The RSF-TD can extract useful features among adjacent pixels of both horizontal and vertical directions with better accuracy. The RSF-TD can be used for detecting tampered image that has undergone multiple tampering. The RSF-TD achieves very good precision, F1-score, and recall performance in comparison with the recent tampering detection method.

The paper is arranged as follows: the proposed resampling feature tampering detection method through CNN is conferred in section 2. The overall outcome achieved using the RSF-TD method over different tampering detection model are given. The last section discusses the significance of RSF-TD and also discusses the future direction of research work.

2. EFFICIENT RSF AND CNN MODEL FOR IMAGE FORGERY DETECTION

Here the tampering detection through resampling feature extraction and CNN descriptor is presented. For detecting tampering and segmenting tampered region efficiently the following design is presented in Figure 1. This RSF-TD architecture is having six steps. First, the image is segmented into different patches. Then, the feature is extracted using a scale-invariant descriptor for establishing the duplicated region even under the small and smooth region.

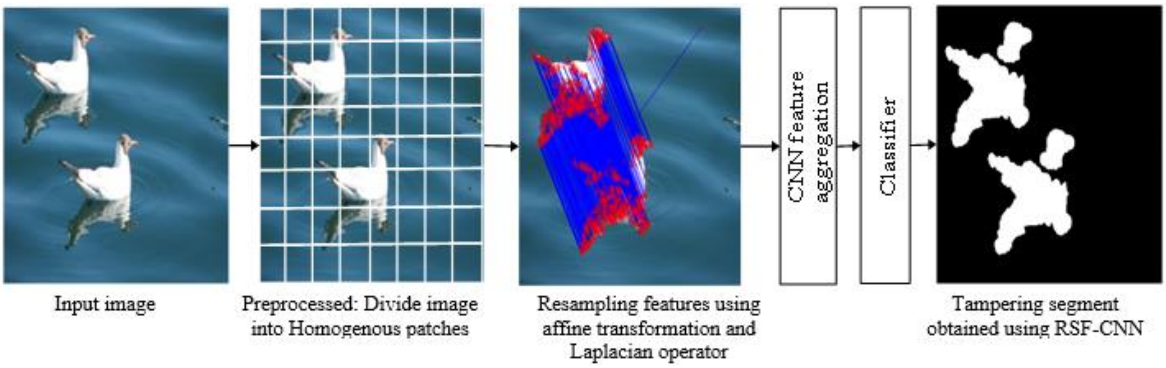

Input image
Preprocessed: Divide image into Homogenous patches
Resampling features using affine transformation and Laplacian operator
CNN feature aggregation
Classifier
Tampering segment obtained using RSF-CNN

Figure 1. Methodology of proposed RSF-CNN Model for tampering detection

2.1. Preprocessing and resampling feature detection and extraction

Generally, the tampered images will have significant impacts on the statistical properties along the edges. Similar to methodologies presented in [29] in this work the resampling feature are extracted through affine transformation and Laplacian function. Here the image is divided into non-overlapping with patch size set to 64. The dimension of the patch will be 64*64 for considering an image size of 512*512. Keeping the size to 512*512 significantly reduce the computation time in detecting and localizing tampering region. To predict the linear error Laplacian function is utilized [13]. Affine transformation matrices are used for collecting the errors considering various directions and angels. Finally, Fourier transformation is used for extracting RSF considering diverse tampering transformation. The existing method performs localization at pixel level; however, the RSF-TD performs localization at the pixel level. Here the patch size is set to 32*32 and block size is kept to 8*8 for extracting local RSF with less redundancy. Once RSF is extracted they are trained using CNN; achieving higher accuracy depends on the order of feature aggregation. The existing model arranges the features in the horizontal or vertical direction; thus, poor correlation among different directions significantly impacts accuracy. To address the aforementioned issues in this space-filling curve [30]-[33] is used. The spacing filling is very effective in converting the multi-dimension problems to a single dimension [34]-[37].

2.2. Aggregation of features and decision using CNN for tampering detection

The previous section extracts efficient RSF features; these features must be cumulated to build an efficient learning mechanism for the classification of the image is undergone hybrid primary attacks. Different aggregation methods are modeled in (1) to (4) [38]. The (1) defines the minimum aggregation model,

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

The (2) defines the maximum aggregation function

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

The (3) defines the mean aggregation function

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

The (4) squared mean aggregation function

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

In (1) to (4), the parameter $G_j = \left[G_{j,1}, \dots, G_{j,D}\right]$ defines the amount of feature extracted in the j^{th} patch and O_q defines the maximum patch size used. In this work we used different pooling methods; then features are aggregated for eliminating spatial dependency. Let θ defines CNN parameter, M defines loss function of CNN structure sued, and G_{agr} defines cumulated features. Then, the gradient of M concerning θ is defined as follows:

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

with,

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

Using (6) we can state that $\mu_{j,k} = 1$ provided $j = k$; otherwise $\mu_{j,k} = 0$. The parameters $j_{\downarrow}(d)$ and $j_{\uparrow}(d)$ define the feature vector with the smallest and largest d^{th} component. Using all pooling together assures that gradient weights can be optimized more efficiently; thus, aiding in achieving better tampering detection accuracy. Finally, the optimized RSF are aggregated for building descriptor G using two-layer fully connected CNN [39]; this assures higher accuracy with minimal computation time.

2.3. Training of CNN

The RSF-TD without the need for any fixed network can be trained end-to-end by using the whole image. Then, the decision is taken to classify image is tampered or not. Here loss functions are backpropagated within the network of respective patches; this helps in obtaining better-correlated features in an adaptive nature. Thus, assures RSF-TD achieves better detection accuracy with less misclassification.

3. RESULTS AND DISCUSSIONS

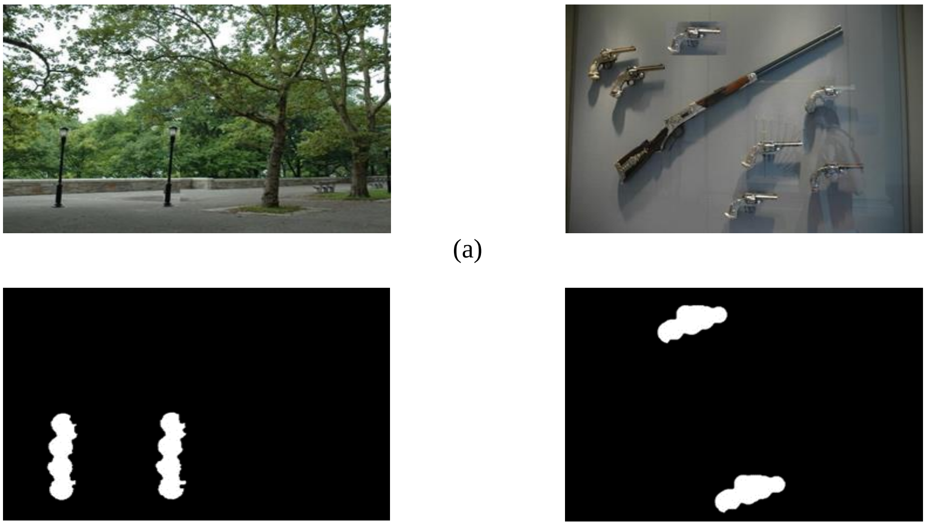
Here experiment is conducted to study the tampering detection outcome of RSF-TD and standard tampering detection methods. The experiment is conducted using window 10 operating system with Intel quad processor and 16 GB Ram. The RSF-TD has been implemented through Matlab, C++, and the Anaconda python 3 frameworks. The experiment is done using two standard datasets such as media integration and communication center (MICC) and D0 dataset because it has undergone a hybrid transformation attack. More detail of the dataset used for the experiment is given in Table 1. The metric used for evaluating the performance of RSF-TD and the existing tampering detection model [40], [41] is recall, F1-score, and false-positive rate.

Table 1. Dataset description

Dataset	Image size	Scaling and rotation	Compression
MICC	600	Yes	No
D0	50	yes	Yes

3.1. Evaluation of performance on MICC dataset

The MICC is composed of 300 genuine images and 300 images undergo a hybrid transformation attack. Therefore, a total of 600 images are available. On average 1.2% of patches are tampered with. Thus, it is extremely difficult in detecting tampering. The Figure 2(a) shows the original image, Figure 2(b) shows respective segmentation outcome using RSF-TD respectively. In Figure 2, the tampering region segmentation outcome achieved using RSF-TD is shown. Similarly, The Figure 3(a) shows the original image, Figure 3(b) shows respective ground truth of tampered region, segmentation outcome achieved using existing and RSF-TD model is shown in Figure 3(c) and Figure 3(d), respectively. Figure 3 shows the segmentation outcome achieved using RSF-TD and the existing segmentation model [26]. Table 2, shows the recall, false positive rate (FPR), and F1-Score performance achieved using RSF-TD and the existing tampering detection model [40]. From the result, we can state the RSF-TD archives have much better detection accuracies under hybrid attack in comparison with existing tampering detection models.



(a)

(b)

Figure 2. The results of the proposed RSF-CNN model; (a) original image and (b) segmentation outcome using RSF-TD

3.2. Evaluation of performance on D0 dataset

In this section performance of RSF-TD and the existing tampering, detection methods are studied using the D0 dataset. The dataset undergoes hybrid transformation such as scaling and rotation with JPEG compression. Thus, tampering detection makes very challenging. The Figure 4(a) shows the original image, Figure 4(b) shows respective ground truth of tampered region, feature extraction and segmentation outcome achieved using existing and RSF-TD model is shown in Figure 4(c), and Figure 4(d), respectively. In Figure 4, the segmentation outcome of the tampered region using RSF-TD is shown. The detection accuracy using RSF-TD and the existing model on D0 dataset is shown in Table 3. Through the outcome achieved we can state that RSF-TD performs significantly better than the existing tampering detection model in terms of F1-score, FPR, precision, and recall.

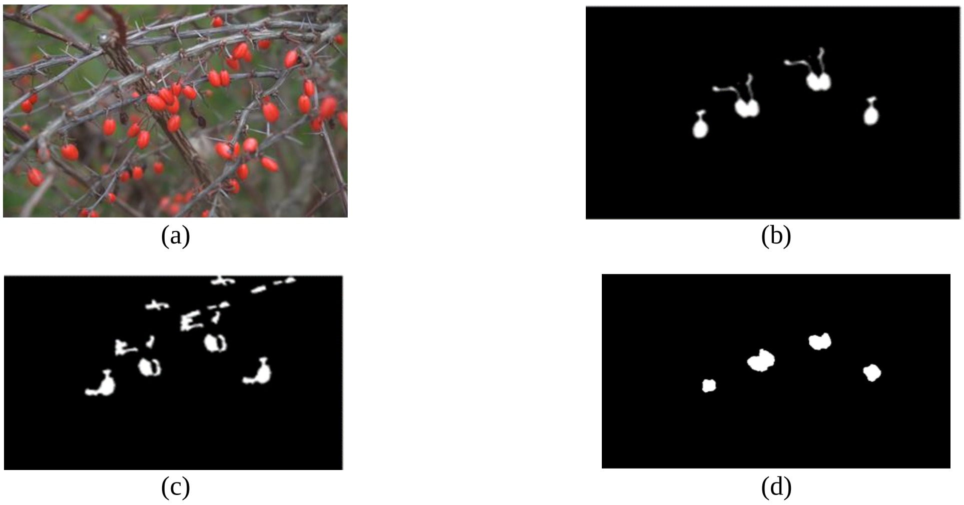


Figure 3. Tampering region segmentation outcome using RSF-TD and existing tampering region segmentation model; (a) original image, (b) ground truth, (c) existing model [26], and (d) RSF-TD

Table 2. RSF-TD and existing method tampering detection accuracy for MICC dataset

Model	Recall/TPR	FPR	F1-Score
Raju and Nair 2018 [40]	89.14	-	92.6
RSF-TD	97.5	1.4	97.7

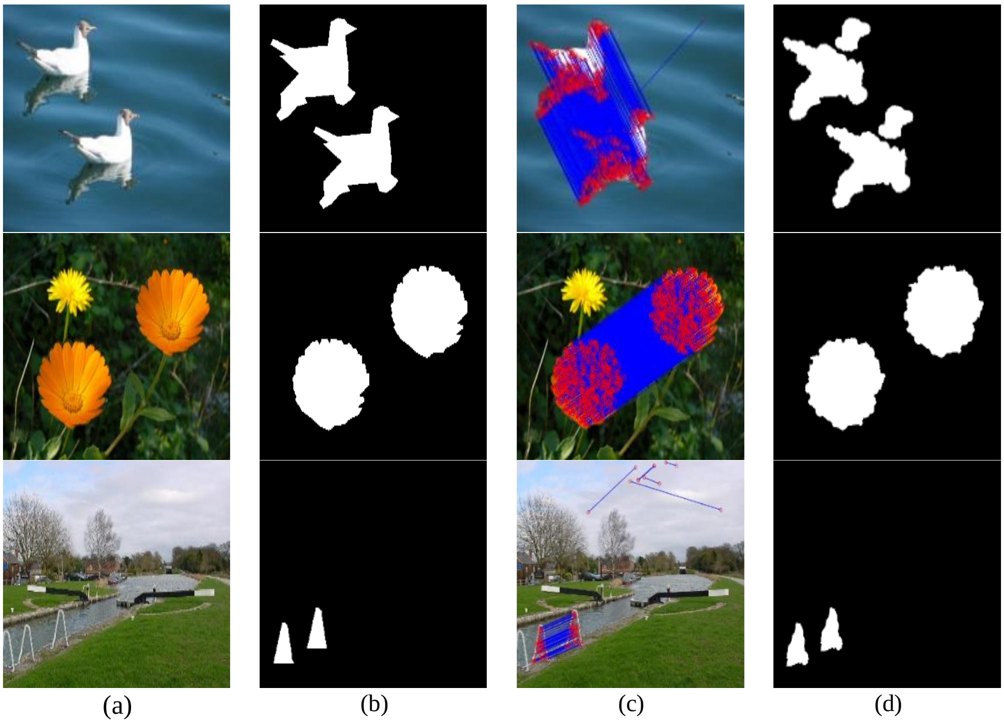


Figure 4. Segmentation outcome of RSF-TD model; (a) input image, (b) ground truth, (c) feature extraction, and (d) segmentation outcome

Table 3. RSF-TD and existing tampering detection model for D0 dataset

Model	Recall	Precision	FPR	F1
Huang and Ciou [41]	84.88	92.81	3.39	88.67
RSF-CNN	98.08	98.84	1.68	99.28

3.3. Computation complexity performance evaluation

Here experiment is done to study the computation complexity of different tampering detection methods. The computation complexity is measured in terms of the amount of time taken to detect tampering regions. Figure 5 shows the computation time taken to process MICC-600 using the deep learning-based method [42], the hierarchical method, and RSF-TD. Similarly, Figure 6 shows the computation time taken to process MICC-2000 using the deep learning-based method [42] and RSF-TD. Figure 7 shows the computation time taken to process the CoMoFoD dataset using the DBSCAN-based method, and RSF-TD. From Figures 5 to 7 we can see the RSF-TD significantly reduces computation time in comparison with the deep learning-based method, hierarchical method, and DBSCAN-based method.

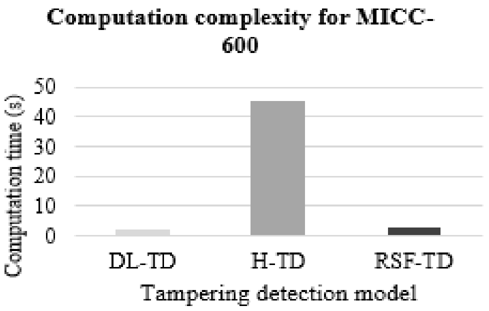


Figure 5. Computation time for MICC-600

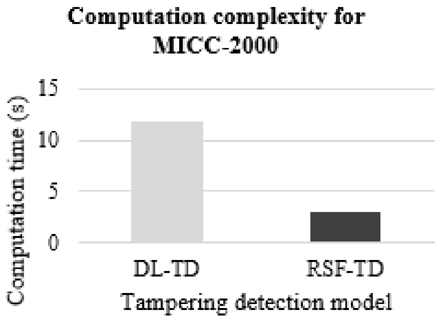


Figure 6. Computation time for MICC-2000

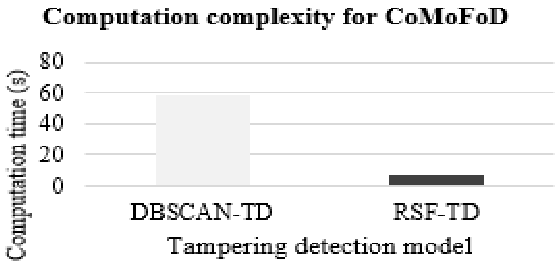


Figure 7. Computation time for CoMoFoD

4. CONCLUSION

Here the paper emphasized using the resampling feature through effective preprocessing and CNN model. The RSF-TD brings in good tradeoffs between achieving higher detection accuracies with minimal computation time. Further, able to achieve higher detection accuracies with better segmentation outcomes in comparison with the standard tampering detection model. The result proves the RSF-TD can extract highly correlated features and eliminate spatial dependencies. The experiment conducted on two datasets with hybrid tampering attack transformation shows the RSF-TD achieves much better accuracies in comparison with the recent tampering detection model which is measured through the following metrics such as F1-score, FPR, TPR, precision, and recall. Despite achieving superior detection accuracies the model can be further improved in the future by eliminating outliers through effective design of CNN framework that is robust against noise. Further, validate the model using more diverse datasets.

REFERENCES

[1] F. Luan, S. Paris, E. Shechtman, and K. Bala, “Deep Photo Style Transfer,” *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 6997-7005, doi: 10.1109/CVPR.2017.740.

[2] N. P. Joglekar and P. N. Chatur, “A Compressive Survey on Active and Passive Methods for Image Forgery Detection,” *International Journal of Engineering and Computer Science*, vol. 4, no. 1, pp. 10187-10190, 2015.

[3] J. Bunk *et al.*, "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning," *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1881-1889, doi: 10.1109/CVPRW.2017.235.

[4] V. Schetinger, M. M. Oliveira, R. DaSilva, and T. J. Carvalho, "Humans are easily fooled by digital images," *Computers & Graphics*, vol. 68, pp. 142-151, 2015, doi: 10.1016/j.cag.2017.08.010.

[5] R. M. Joseph and A. S. Chithra, "Literature survey on image manipulation detection," *International Research Journal of Engineering and Technology (IRJET)*, vol. 2, no. 04, pp. 740-744, 2015.

[6] M. T. Shashidhar and K. B. Ramesh, "A novel framework for optimized digital forensic for mitigating complex image attacks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 5198-5207 2020, doi: 10.11591/ijece.v10i5.pp5198-5207.

[7] H. Li, W. Luo, X. Qiu, and J. Huang, "Image Forgery Localization via Integrating Tampering Possibility Maps," in*IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1240-1252, May 2017, doi: 10.1109/TIFS.2017.2656823.

[8] A. Pourkashani, A. Shahbahrami, and A. Akoushideh, "Copy-move forgery detection using convolutional neural network and K-mean clustering," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 11, no. 3, pp. 2604-2612, 2021, doi: 10.11591/ijece.v11i3.pp2604-2612.

[9] J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. S. Manjunath, "Exploiting Spatial Structure for Localizing Manipulated Image Regions," *2017 IEEE International Conference on Computer Vision (ICCV)*, 2017, pp. 4980-4989, doi: 10.1109/ICCV.2017.532.

[10] L. Bondi, S. Lameri, D. Güera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering Detection and Localization Through Clustering of Camera-Based CNN Features," *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1855-1864, doi: 10.1109/CVPRW.2017.232.

[11] R. Thakur and R. Rohilla, "Recent advances in digital image manipulation detection techniques: A brief review," *Forensic Science International*, vol. 312, 2020, doi: 10.1016/j.forsciint.2020.110311.

[12] Y. Liu, Q. Guan, X. Zhao, and Y. Cao, "Image forgery localization based on multi-scale convolutional neural networks," *IH&MMSec '18: Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 2018, pp. 85-90, doi: 10.1145/3206004.3206010.

[13] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, no. 2, pp. 180-189, 2007, doi: 10.1016/j.forsciint.2006.11.002.

[14] W. Wang, J. Dong, and T. Tan, "Exploring DCT Coefficient Quantization Effects for Local Tampering Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1653-1666, Oct. 2014, doi: 10.1109/TIFS.2014.2345479.

[15] 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*, vol. 31, no. 1, pp. 57-71, 2013, doi: 10.1016/j.imavis.2012.09.002.

[16] A. Gupta, "New Copy Move Forgery DetectionTechnique Using Adaptive Over-segmentation and Feature Point Matching," *Bulletin of Electrical Engineering and Informatics (BEEI),* vol. 7, no. 3, pp. 345-349, 2018, doi: 10.11591/eei.v7i3.754.

[17] I. B. K. Sudiatmika, F. Rahman, Trisno, and Suyoto, "Image forgery detection using error level analysis and deep learning," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control),* vol. 17, no. 2, pp. 653-659, 2019, doi: 10.12928/TELKOMNIKA.v17i2.8976.

[18] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 3431-3440, doi: 10.1109/CVPR.2015.7298965.

[19] 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.

[20] 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,* 2016, pp 5-10, doi: 10.1145/2909827.2930786.

[21] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016, pp. 1-6, doi: 10.1109/WIFS.2016.7823911.

[22] Y. Zhang, J. Goh, L. L. Win, and V. L. Thing, "Image region forgery detection: A deep learning approach," *In Proceedings of the Singapore Cyber-Security Conference (SG-CRC),* 2016, vol. 14, pp. 1-11, doi: 10.3233/978-1-61499-617-0-1.

[23] V. T. Manu and B. M. Mehtre, "Visual artifacts based image splicing detection in uncompressed images," *2015 IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS)*, 2015, pp. 145-150, doi: 10.1109/CGVIS.2015.7449911.

[24] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," in *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 3, pp. 507-518, March 2015, doi: 10.1109/TIFS.2014.2381872.

[25] V. Badrinarayanan, A. Kendall, and R. Cipolla, "SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 12, pp. 2481-2495, Dec. 2017, doi: 10.1109/TPAMI.2016.2644615.

[26] S.-J. Ryu and H.-K. Lee, "Estimation of linear transformation by analyzing the periodicity of interpolation," *Pattern Recognition Letters*, vol. 36, pp. 89-99, 2014, doi: 10.1016/j.patrec.2013.09.028.

[27] B. Mahdian and S. Saic, "Blind Authentication Using Periodic Properties of Interpolation," in *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 529-538, Sept. 2008, doi: 10.1109/TIFS.2004.924603.

[28] D. Voorhies, "Space-filling curves and pace-filling curves and a measure of coherence," *Graphics Gems II,* pp. 26-30, 1991, doi: 10.1016/B978-0-08-050754-5.50018-9.

[29] B. Moon, H. V. Jagadish, C. Faloutsos, and J. H. Saltz, "Analysis of the clustering properties of the Hilbert space-filling curve," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 13, no. 1, pp. 124-141, Jan.-Feb. 2001, doi: 10.1109/69.908985.

[30] T. M. Mohammed *et al.*, "Boosting image forgery detection using resampling detection and copy-move analysis," *Society for Imaging Science and Technology*, vol. 7, pp. 118-1-118-7, 2018, doi: 10.2352/ISSN.2470-1173.2018.07.MWSF-118.

[31] 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)*, 2017, pp. 2152-2156, doi: 10.1109/ICASSP.2017.7952537.

[32] 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, 2019, doi: 10.1109/ACCESS.2019.2956508.

[33] 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)*, 2020, pp. 571-576, doi: 10.1109/ICACCS48705.2020.9074408.

[34] A. Kuznetsov, “Digital image forgery detection using deep learning approach,” *Journal of Physics: Conference Series*, vol. 1368, no. 3, 2019, doi: 10.1088/1742-6596/1368/3/032028.

[35] R. Huang, F. Fang, H. H. Nguyen, J. Yamagishi, and I. Echizen, “A Method for Identifying Origin of Digital Images Using a Convolutional Neural Network,” *2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2020, pp. 1293-1299.

[36] A. Flenner, L. Peterson, J. Bunk, T. M. Mohammed, L. Nataraj, and B. S. Manjunath, “Resampling Forgery Detection Using Deep Learning and A-Contrario Analysis,” *Society for Imaging Science and Technology*, vol. 7, pp. 212-1-212-7, 2018, doi: 10.2352/ISSN.2470-1173.2018.07.MWSF-212.

[37] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, “A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection,” in *IEEE Access*, vol. 8, pp. 133488-133502, 2020, doi: 10.1109/ACCESS.2020.3009877.

[38] C. Pun, X. Yuan, and X. Bi, “Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching,” in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1705-1716, Aug. 2015, doi: 10.1109/TIFS.2015.2423261.

[39] A. Kuznetsov and V. Myasnikov, “A new copy-move forgery detection algorithm using image preprocessing procedure,” *Procedia Engineering*, vol. 201, pp. 436-444, 2017, doi: 10.1016/j.proeng.2017.09.671.

[40] P. M. Raju and M. S. Nair, “Copy-move forgery detection using binary discriminant features,” *Journal of King Saud University - Computer and Information Sciences*, 2018, doi: 10.1016/j.jksuci.2018.11.004.

[41] H-Y. Huang and A-J. Ciou, “Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation,” *EURASIP Journal on Image and Video Processing*, vol. 68, 2019, doi: 10.1186/s13640-019-0469-9.

[42] M. Bilal, H. A. Habib, Z. Mehmood, T. Saba, and M. Rashid “Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering,” *Arabian journal for science and engineering*, vol. 45, pp. 2975-2992, 2019, doi: 10.1007/s13369-019-04238-2.

BIOGRAPHIES OF AUTHORS

Manjunatha S is a Research Scholar at JSSATE Research Centre, Dept. of CSE, JSSATE, affiliated to VTU Belagavi. He completed M. Tech Computer Science and Engineering from NMAMIT Nitte Mangalore, affiliated to VTU Belagavi, Karnataka. Now he is working as an Associate Professor Dept. Of ISE, Global Academy of Technology, Bengaluru. He can be contacted at email: manjunaths@gat.ac.in.

Dr. Malini M. Patil is presently working as an Associate Professor in the Department of Information Science and Engineering at J.S.S. Academy of Technical Education, Bangalore, Karnataka, India. She received her Ph.D. Degree from Bharathiar University in the year 2015. Her research interests are big data analytics, bioinformatics, cloud computing, image processing. She has published more than 50 research papers in reputed peer-reviewed international journals. She is a member of IEEE, IEI, ISTE, CSI. She has attended and presented papers in many international conferences in India and Abroad. Presently she is guiding 3 research scholars and one research scholar has completed the Ph.D. He can be contacted at email: drmalinimpatil@gmail.com.