Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).
IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) | 978-1-6654-1960-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICICV50876.2021.9388471

Deep learning-based Technique for Image Tamper Detection

Manjunatha. S
Department of Information Science & Engineering.
Global Academy of Technology
Bengaluru, 560 098, India
manjunaths.dvg@gmail.com

Malini M Patil
Department of Information Science & Engineering.
J S S Academy of Technical Education
Bengaluru, 560 060, India
drmalinimpatil@gmail.com

***Abstract*- The objective of the research work is to thoroughly study existing methodologies for detecting passive image tampering using deep learning techniques. Here, survey is conducted predominantly focusing on tampering detection using deep learning techniques. Different image tampering datasets such as MICC, CASIA, and UCID, etc. have been used by existing tampering detection methodologies for validating tampering detection accuracies. From the study, it is identified that not all method obtains good accuracies for all kind of attack such as splicing, compression, rotation, resampling, copy-move, etc. From the study it is identified for detecting tampering efficiently it is important to design an efficient deep learning-based feature extraction mechanism that learns correlation among pixels more efficiently. In contrast with another recent survey, this paper covers significant developments in passive image forensic analysis methods adopting deep learning techniques. Existing methodologies are studied concerning benefit, limitation, the dataset used, and kind of attack considered. The paper further highlights future challenges and open issues, and also provides the possible future solution in building efficient tampering detection mechanism using deep learning technique. Experiment outcomes show good performance in connection with TPR, FPR, and F1-Score.**

Keywords—Image forgery, Machine Learning, CNN, Deep Learning, Neural Network.

I. INTRODUCTION

Manipulated images are presented in such a manner that it is almost impossible to visually discriminate forged data from the original data. It has a noteworthy role in uploading and downloading images to those social media like SNS (Social Network Service), Facebook, WhatsApp, and Instagram. Due to this, it is very challenging to differentiate between the actual image and the tampered image which is created by using available tools. The fields like forensics, industrial photography, e-commerce, and medical imaging, and substantiating the uniqueness of images is a major challenge. Detecting traces of manipulation of the image is an exciting task and relatively difficult to declare images are trustworthy. Hence, the determination in enhanced image manipulation detection cannot be ignored. Traditional approaches for image manipulation detection typically uses handcrafted structures. The major problem with these methods is the procedures can categorize a particular type of manipulation by recognizing a definite feature in that image. Image manipulation can be found in several fields like photography, news media, arts, and the medical field, etc. So the major concern in this society is claiming medical insurance with forged medical images and also it may lead to false treatment. Hence, the determination in improved image forgery detection cannot be overlooked. In image composition, various techniques like copy-move, splicing, etc., are the most widespread manipulation practices that are found in [1], [2], and [3]. These practices encompass a merged image of two or more sections that create an altered image. Figure.1 shows three different examples of an original image and its respective altered image.

a.) Original image b.) Tampered image

Fig. 1. Example of image tampering.

The statement of the intended alteration of facts restricted in the digital image to conceal it or modify it will be called as attacks. The most common categories of non-natural distortions of digital images are splicing [3], copy-move [1,2], and resampling [4]. All of them are used to conceal the geometric transformation existing in the digital image. The copy-move1 type of distortion means photocopying a section of a digital image, presenting any distortion into this fragment, and implanting the modified fragment into another area of the same image. The most common type of imitation alterations is the resampling-geometric conversion of image chunks and implanting those into other images. The other usually used type of distortions is splicing and this will use fragments of diverse digital images to create a detailed distortion of an existing one or a new image. And finally, an alternative way

that attackers use is JPEG compression [5]. In this, after implanting any info in the JPEG file and recompression, there are native transformations in the belongings of JPEG compression. The pronounced procedures of implanting alterations are the most common today, as shown by the enormous amount of publications aimed at evolving solutions to detect such attacks. To find an answer to these issues, the researchers have suggested some methodologies that can be categorized into Active and Passive technologies [6-8] as shown in Figure.2.

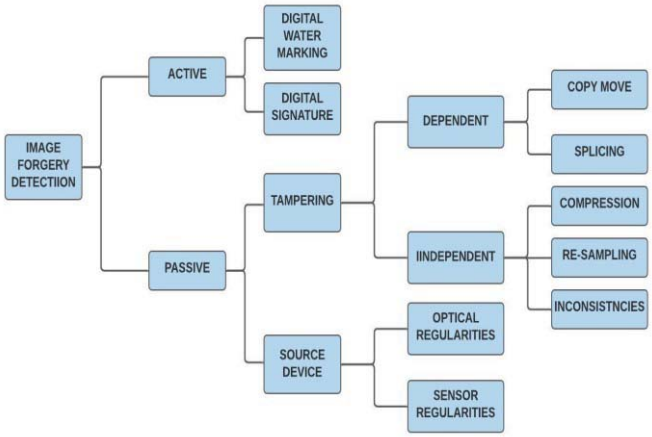

Fig. 2. Classification of Image forgery detection approaches [9]

This work predominantly focuses on carrying out a survey of passive image tampering attack detection methodologies using deep learning techniques. Further, the research identifies the research problem and present a possible solution in detecting diverse image tampering attack using deep learning technique.

The contribution of the research is as follows.

- No prior work has considered surveys specific to passive attacks using the deep learning technique.
- Further, the research work presents a possible futuristic solution.
- Presented an image tampering detection method using resampling feature and convolution neural network.

II. LITERATURE SURVEY

In recent times, the attentiveness about Deep Learning (DL) has increased and many remarkable results are evolving. Hence, forensic researchers try to apply DL to perceive the manipulation of images without human intrusion [13]. Advancement of the technology in the graphics processing unit and achievement of DL practices [15] in computer vision, inspired a group of researchers to relate all available DL models for image manipulation detection. These DL chains feature extraction and classification steps. This procedure is data-driven and accomplished by spontaneously learning complex and abstract structures, essential to detect interfered regions. It saves the energy and time needed to discover native features of interfered digital images. On the other hand, the training of DL models is inflexible and requires great computational power with an enormous size of data. The initiation of data-driven results established a substantial leap in execution and assured a broad view. Procedures were created using ML [16] to mine the proper native features of the digital image in both spatial and transform domains, which are used to train a classifier. Extract all the landscapes from the digital image that permits uninterrupted and consistent image forgery detection. In its place, localization can be attained by running in sliding-window modality and by proper confined score. These supreme discriminating features depend on high-order indicators of an image which is going to help enlightening spatial irregularities created with the help of the existence of imitations.

In the present modern era, DL based approaches have become more important. Some initial papers, encouraged by the achievement of residual-based ML approaches, recommended CNN architectures, predestined to mine residual feature records. For digital image forgery detection, there are some models available in Deep Learning, like Convolutional Neural Networks (CNN), Deep Neural Network (DNN), and Recurrent Neural Network (RNN). Among those, CNN is the most common DL models. The convolution layer of CNN will perform as a discriminator and have an extractor. CNN's abstract features support the state of the image instead of extracting the features of the altered image. The google trends are depicted in the following Fig. 3. It is observed that the literature survey relating to the publications on image forgery detection using deep learning methods are very sparse.

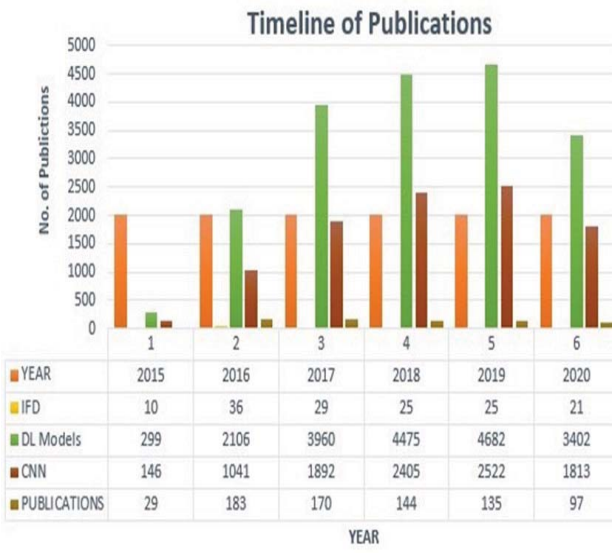

Fig. 3. Timeline of Publications from 2015 to 2020 [17].

In [18], recommended a two-step DL approach to learn features and a mechanism that detects manipulated digital images that may be in dissimilar image formats. Within the initiative, they separate the images into areas then the Loaded Auto-encoder model is employed to find out the structures for every spot. Within the next step, the appropriate data is added to every spot to urge precise consequences. And they have also suggested doing it by using other deep learning architectures such as DBN it can improve the performance. In [19], suggesting a unique CNN-based IFD technique that can automatically learn how image altering can be done. The convolutional layer in this acquires image alteration features by destroying the content of the image. This convolution layer studies local operational association among pixels rather than seeing the content of a picture since tampering alters some resident associations, it detects several tampering in an image. The main issue in the detection process is that frequent attacks cannot give conventional results. Additionally, to trace the

interfered area, the majority of the effort is concluded by pointing the JPEG images, which means that the altered section is noticed using evidence left by several actions of JPEG compression.

In [20] suggested the response to concentrate image splicing with the help of Multi-Task Fully Convolutional Network. It is proved that Multi-Task Fully Connected Network attains better demonstration than single-task Fully Connected Network because single-task Fully Connected Network delivers irregular output for localization for limited cases. These authors also suggested Multi-Task Fully Convolutional Network with a set of output branches. Among these, one branch is engaged to acquire the surface label information, and the next one is engaged to acquire the interfered section edge. Better performance can be achieved even this process has been exposed to show the degradation among post-processing techniques.

In [21] suggested CNN for a multi-domain-based approach which is a combination of both special and frequency domains. This can use to categorize and limit single, uncompressed, and double compressed sections of images. The Spatial domain-based CNNs takes an input of n*n sized areas of RGB channels. And it is collected of both convolutional chunks and a set of fully connected layers. The Frequency domain-based CNN takes DCT coefficients of an area as input. The Frequency domain-based CNN's encompasses both the layers trailed by a set of pooling layers with all three full links. The Multi-domain CNN links the output approaching from fully associated layers of both networks and this will categorize the areas into one among all classes, double compressed or uncompressed. From this work, we can notice that median filtering from a digital image is remarkably exciting work.

In [22], suggested a Convolutional Network Networks based approach will mine median filtering residuals in the digital images to handle the several challenges. The primary layer in Convolutional Network Networks may be the filter layer which will condense all interference that arises because of the existence of the textures and edges. This exclusion of intervention supports the model to examine all the hints left by median filtering.

In [23], offered a CNN-based method to detect interfering were the hints left by various camera models, which abstracts the features regarding the camera model from digital image reinforcements. The Clustering system is employed to study the mined structures and this will classify the digital image as either artificial or not. In [24], the author suggested using noise residual structures for image manipulation detection with localization. CNN is used meant for mining the noise remaining centered landscapes of the digital image and the SVM is used for classifications.

In paper [25], suggested CNN for digital image forgery detection in copy-move and another one image splicing. The primary convolution layer on CNN is involved in preprocessing operations to search for concerns formed by altering processes. Here, the CNN was trained with characterized path illustrations from training images. After this pre-trained CNN was applied on trial images and for the detection of tampering SVM classifier is used.

In [26], the authors proposed a way to perceive copy-move forgery, i.e., two branch DNN architecture called BusterNet, this is having the capacity of making alteration concealment.

In DNN, the first branch is employed for the recognition of manipulated sections that accepts an image as an input, mining all the features by using CNN, by using Mask Decoder the upsamples feature map is created and a binary classifier is used to create a mask. Therefore, the next branch is employed to detect the emulated sections which take the image as an input and it uses the CNN for mining the features. The Self-Correlation component to appear the features resemblance, to accumulate the suitable statistics the Percentile Pooling is used. Then this synthesis module takes input through two branches and creates the ultimate copy-move forgery calculation.

Bi et al. [27], are recommended a CNN-based method called RRU-Net (Ringed Residual U-Net,) where it is an end-to-end image segmentation network, for digital image splicing detection. The RRU-Net goals to develop the learning approach of CNN over recollection and association with the human brain mechanism. The outstanding propagation is engaged to remember the input feature info to unravel the ruin issue within a deeper network. Finally, the remaining response merges the response feature info to discriminate against the original and fake regions. This RRU-Net tested on two very popular datasets i.e., CASIA and COLUMBIA.

Wang et al. [28], A novel model is employed to detect and also to locate the image manipulations. This novel method was tested on two datasets i.e., Columbia and Cover. This method was skilled to find equally a copy-move and also splicing falsifications.

Amit Doegar, et al, [29], is proposed to utilize the CNN based pre-trained AlexNet model's deep structures without devoting much time to training. The suggested approach also exploits the SVM as a classifier. The performance of these deep features mined from that proposed model is satisfactory, even in the occurrence of geometrical and rotational transformation. Summary of Several DL Models in Image Forgery Detection is shown in Table.1.

In the next section, the possible solution to overcome issues of existing tampering detection method using deep learning technique is discussed.

III. Possible Solution for Image Tampering Detection

Recent image tampering work shows using deep learning techniques such as CNN aid in improving tampering detection accuracies. However, existing tampering detection methodologies predominantly focused on identifying a particular type of manipulations such as splicing, resampling, copy-move, etc. As a result, some method works well for detecting one kind of attack; however, fails to detect another kind of hybrid attack such as introducing resampling attack of copy-move tampered segment. Along with that, it is practically a difficult task to know the tampering type in advance. Then, segmenting only the tampering region is very difficult; especially when there exist multiple forgeries of similar patterns within an image. CNN in object segmentation have attained the very good result; CNN extracts hierarchical feature from the different level to segment meaningful shape of respective objects. Contrasting with meaningful segmentation, the tampered segment can be copied segment for other portion of an image or it could be a removed object within an image. a well-crafted tampered image generally exhibits a good correlation between the authentic and tampered image. Thus, for detecting tampering and segmenting tampered region efficiently the following design is presented in Fig. 4.

Article-No.	Type of Tampering	Features, Model & # Layers	Data Set	Pros/Cons	Remarks
[18]	Cut-paste, Copy-move	Three-level, 2-D Daubechies wavelet decomposition & SAE Stacked Autoencoders	CASIA v1.0, CASIA v2.0, and Columbia	Advantage: 1. It will characterize tampered regions across JPEG and TIFF image formats. Disadvantages: 1. The interfered areas must be manually recognized. 2. The interfered areas are not precisely detected.	Accuracy 91.09%
[19]	Gaussian blurring, Median filtering, Resampling AWGN,	Prediction error filters & CNN – 8 layers	Different images from 12 distinct camera models	Advantage: 1. The projected CNN-based forgery detection technique will automatically learn and have very good accuracy.	Accuracy 99.10%
[20]	Image Splicing	Surface probability & edge probability map & MFCN (Multi-task fully convolution network)	CASIA v1.0, CASIA v2.0, Columbia and Carvalho	Advantage: 1. The projected approaches outperform present splicing localization methods. Disadvantages: 1. They used the trained model to assess images, which are not in the training set.	0.61 (Columbia) MCC Score 0.52 (CASIA v1.0) & F1-Score 0.54 (CASIA v1.0) 0.47 (Columbia)
[21]	JPEG Double compression, Cut-paste	Histogram & RGB Features of DCT and Multi-domain CNN	UCID (1338 Images)	Advantage: 1. The planned technique explores CNN abilities to categorize and localize the compressed patches of images Disadvantages: 1. They fail to explore the CNNs to perceive various types of compressions	Accuracy 95%
[22]	Median filtering and Cut-paste	Median filter residuals & the CNN with 9 layers	BOSS base 1.01, UCID, NRCS Photo Gallery, Dresden, BOSS RAW (15352 images)	Advantage: 1. The outcomes show that the the suggested technique attains significant performance improvements. Disadvantages: 1. It is limited to recognize cut-and-paste imitations only.	Accuracy 85.14%
[23]	Cut-paste	Camera model features & CNN – 11 layers	Dresden Image Database (16 thousand images from 26 distinct cameras)	Advantage: 1. The presented algorithm exploits the CNN to mine features apprehending camera model hints from image spots Disadvantages: 1. They failed to find the traces of camera models and localizations.	Accuracy 81% (Detection) Accuracy 82% (Localization)
[24]	Cut-paste	Noise residual landscapes & Autoencoder	Images were taken from 7 electronic devices & 6 smartphones	Advantage: 1. The proposed method shows decent robustness against distinctive social net post-processing.	F-Measure 0.41(basic) and 0.37 (with post-processing)

			a camera	Disadvantages: 1. They have not achieved a deep investigation of the several degrees of freedom of the autoencoder configuration.	
[25]	Cut-paste, Copy-move	Hierarchical representation through color Images & CNN – 10 layers	CASIA v1.0, CASIA v2.0, and Columbia gray DVMM	Advantage: 1. It mined compressed features of test images, and a feature fusion technique is combined to obtain the result with very good accuracy. Disadvantages: 1. Increased computational complexity	Accuracy 98.04%
[27]	Cut-paste	Image residuals & RRU-Net	CASIA, COLUMB	Advantage: 1. They attained the tamper detection without any pre-processing & post-processing Disadvantages: 1. They have not visualized the latent discriminative feature between interfered and un-tampered sections.	Accuracy 76%
[28]	Cut-paste, Copy-move	ResNet-101 & Mask R-CNN	Cover, Columbia	Advantage: 1. It has superior performance over other state-of-the-art image tampering detection approaches Disadvantages: 1. Fail to follow the perfect and comprehensive contours of the unique tamper area.	Avg precision 93% for Cover and 97% for Columbia
[29]	Combinations of geometrical and transformations attacks to the original image	CNN - pre-trained AlexNet Model	Dataset MICC-F220	Advantage: 1. They exploited the SVM as a classifier with the best accuracy. Disadvantages: 1. Not more suitable for all data sets	Accuracy 93.94%

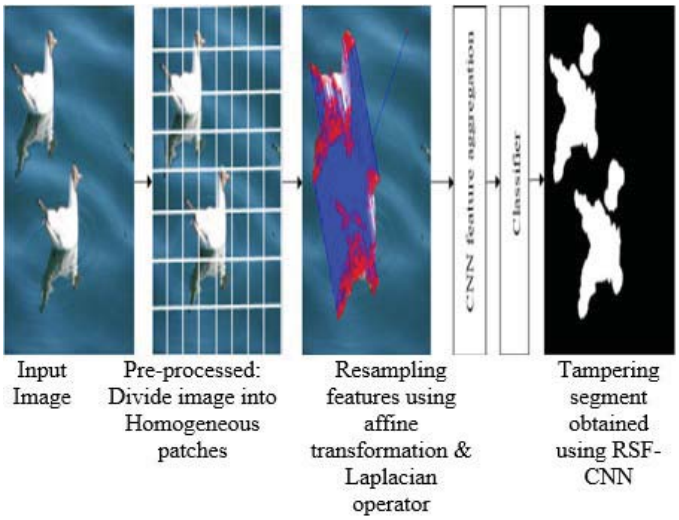

Fig.4. Proposed CNN-based tampering detection methodologies.

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. Generally, the tampered image exhibit certain noises such as compression, resampling, etc. which could be efficiently understood using resampling features. However, using resampling features exhibit periodic correlations between the pixels; this is because of interpolation. The CNN is robust to translation for capturing noisy information using resampling features and generating spatial maps among a different segment of an image; thus both are utilized for localizing tampered segments. Thus, the resampling feature will be estimated for detecting inconsistencies in the estimated resampling factors using improved CNN architecture [33].

IV. Result and Discussion

Here experiment is carried out to assess the performance of the suggested CNN-based tampering detection method over existing tampering detection methods. The proposed model is implemented using python and C++ framework. An experiment is conducted on a complex manipulation dataset namely MICC-600. The dataset is composed of 600 tampered images which are composed of resampling with scaling and rotation.

The tampering outcome achieved using the proposed CNN-based method is shown in Fig. 5. The left side indicates the actual image and the right side indicates corresponding segmentation outcomes. The tampering outcome achieved using proposed and existing methodologies are shown in Fig. 6. From the Figure, it can be seen existing method are not efficient in detecting multiple tampering and achieves very poor segmentation outcomes. The existing tampering detection methodology achieves a Recall/TPR and F1-Score performance of 89.14% and 92.6% respectively. Similarly, the CNN-based tampering detection method achieves a Recall/TPR, FPR, F1-Score performance of 97.5%, 1.4%, and 97.7%, respectively. From the result achieved we can see that

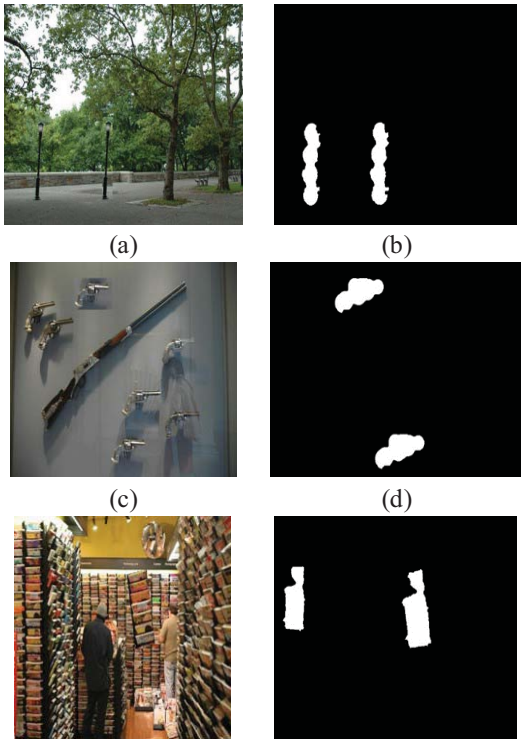

Fig. 5. The outcome was achieved using the proposed CNN-based tampering detection method.

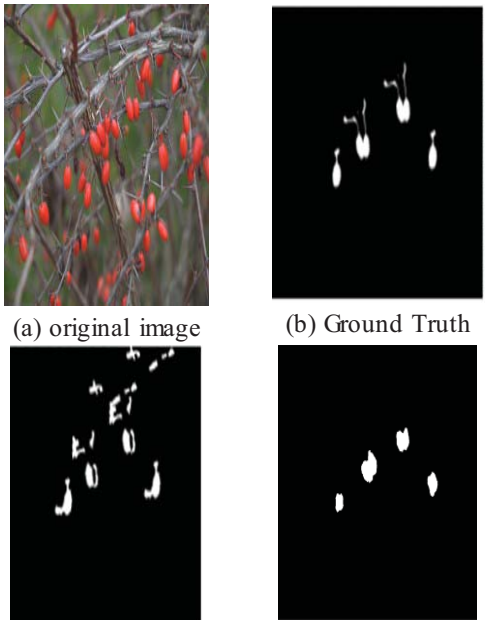

Fig. 6. Comparative analysis of proposed RSF-CNN based tampering detection method over existing tampering detection methodology.

V. CONCLUSION

This article presented a review of Deep learning models for digital image forensics to identify the tampering done on the digital images. The work is organized in such a way that it enables a fundamental base of regimented references. The practices studied in this article are Median filtering, Gaussian blurring, copy-move, Resampling, JPEG Double Compression, and cut-paste. In most of the research articles, the researchers specified that image tampering detection is a very convoluted procedure due to the availability of several software packages. All features are highly delicate to operations in the interfering process. So feature in the image tampering process is playing a crucial role in the process of tamper detection. DL-based approaches have been exposed to be capable to learn abstract and multifaceted landscapes, essential in place of proof of identity of altered sections, automatically. In computer vision, modern improvements in semantic tampering detection procedures are based on CNN and RNN. CNN is applied to explore the content of the substances and outline of a section by mining the categorized features at diverse intensities. During object detection and segmentation, CNNs based architectures reveal the favorable performance in appreciative chromatic notions by evaluating the content of altered sections. And also found that counter-forensic approaches are also being widely used and reveal adequate outcomes. Accordingly, the localization of altered sections with only CNNs based architecture may not be the best tactic. Thus, for detecting tampering and segmenting tampered region efficiently by considering some procedural assumptions. As CNN unveils strong translational invariant to produce spatial maps for the altered sections of an image. Using these features, the CNN model is trained and performance is evaluated using the MICC dataset. Experiment outcome shows the proposed CNN-based tampering detection methodologies are very efficient in detecting multiple tampering with high efficient segmentation outcome when compared with state-of-art tampering detection methodologies. The RSF-CNN based tampering detection methodologies can effectively segregate authenticated and manipulated segments. Future work would consider the present mathematical model of the proposed design and evaluate the model considering a more diverse tampering dataset.

ACKNOWLEDGMENT

Both the authors acknowledge the Global Academy of Technology and JSSMVP's JSSATE Bengaluru for providing the facilities to carry out the research work.

REFERENCES

[1] R. Dixit, R. Naskar, and A. Sahoo. Copy-move forgery detection exploiting statistical image features, 2017 International Conference on Wireless Communications, Signal Processing, and Networking (WiSPNET), Chennai, 2017, pp. 2277-2281.

[2] A. J. Fridrich, B. D. Soukal, and A. J. Luk s, Detection of copy-move forgery in digital images, in Proceedings of Digital Forensic Research Workshop, Citeseer 2003.

[3] B. Patil, S. Chapaneri, and D. Jayaswal. Improved image splicing forgery localization with first digits and Markov model features, IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Srivilliputhur, 2017, pp. 1-5.

[4] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of re-sampling. IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 758–767, 2005.

[5] Bo Liu, Chi-Man Pun, and Xiao-Chen Yuan. Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies. Hindawi Publishing Corporation, Scientific World Journal. http://dx.doi.org/10.1155/2014/230425.

[6] Arun Anoop M, "Image forgery and its detection: A survey," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-9.

[7] Nikhil Kumar P. Joglekar1, Dr. P. N. Chatur. A Compressive Survey on Active and Passive Methods for Image Forgery Detection, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 1 January 2015, Page No. 10187-10190.

[8] Gajanan K. Birajdar, Vijay H. Mankar. Digital image forgery detection using passive techniques: A survey. Digital Investigation. https://doi.org/10.1016/j.diin.2013.04.007.

[9] Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, Kim-Kwang Raymond Choo, Copy-move forgery detection: Survey, challenges and future directions, Journal of Network and Computer Applications, Volume 75, 2016, Pages 259-278, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.09.008

[10] Pradyumna Deshpande and Prashasti Kanikar, Pixel Based "Digital Image Forgery Detection Techniques", International Journal of Engineering Research and Applications, 2012, Vol. 2, Issue 3, Pp. 539-543.

[11] Henry Farid. Image Forgery Detection. IEEE Signal Processing Magazine, March 2007.

[12] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3948-3959, Oct. 2005, DOI: 10.1109/TSP.2005.855406.

[13] Ying Zhang, Jonathan Goh, Lei Win, and Vrizlynn Thing. Image Region Forgery Detection: A Deep Learning Approach. Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016. DOI:10.3233/978-1-61499-617-0-1.

[14] Belhassen Bayar and Matthew C. Stamm. A Deep Learning Approach to Universal Image Manipulation Detection Using A New Convolutional Layer. IH & MMSec 2016, June 20-23, 2016, Vigo, Spain. DOI: http://dx.doi.org/10.1145/2909827.2930786.

[15] 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: Cyber-Security by Design, volume 14, page 1, 2016.

[16] Dheeraj D., Prasantha H.S., "Study of Machine Learning Vs Deep Learning Algorithms for Detection of Tumor in Human Brain," International Journal of Computer Sciences and Engineering, Vol.8, Issue.1, pp.57-63, 2020

[17] https://trends.google.com/trends/explore? Last visited on 6th October 2020.

[18] Ying Zhang, Jonathan Goh, Lei Win, and Vrizlynn Thing. Image Region Forgery Detection: A Deep Learning Approach. Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016; 1 – 11.

[19] Belhassen Bayar, Matthew C. Stamm. A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer. ACM. ISBN 978-1-4503-4290-2/16/06.

[20] Ronald Salloum, Yuzhuo Ren, and C.-C. Jay Kuo. Image Splicing Localization Using A Multi-Task Fully Convolutional Network (MFCN). arXiv:1709.02016v1 [cs.CV] 6 Sep 2017.

[21] Irene Amerinia, Tiberio Uricchioa, Lamberto Ballana, Roberto Caldellia. Localization of JPEG double compression through multi-domain convolutional neural networks. IEEE Conference on Computer Vision and Pattern Recognition Workshops 2017. DOI 10.1109/CVPRW.2017.233.

[22] Jiansheng Chen, Xiangui Kang, Ye Liu, and Z. Jane Wang. Median Filtering Forensics Based on Convolutional Neural Networks. 1850 IEEE Signal Processing Letters, Vol. 22, No. 11, November 2015.

[23] 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), Honolulu, HI, 2017, pp. 1855-1864, DOI: 10.1109/CVPRW.2017. 232.

[24] D. Cozzolino and L. Verdoliva. Single-image splicing localization through autoencoder-based anomaly detection, 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, 2016, pp. 1-6, DOI: 10.1109/WIFS.2016.7823921.

[25] 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), Abu Dhabi, 2016, pp. 1-6, DOI: 10.1109/WIFS.2016.7823911.

[26] Yue Wu, Wael Abd-Almageed, Prem Natarajan. BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization. Proceedings of the European Conference on Computer Vision (ECCV), 2018, pp. 168-184.

[27] X. Bi, Y. Wei, B. Xiao, and W. Li, "RRU-Net: The Ringed Residual U-Net for Image Splicing Forgery Detection," 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 2019, pp. 30-39, DOI: 10.1109/CVPRW.2019.00010.

[28] Xinyi Wang, He Wang, Shaozhang Niu, and Jiwei Zhang. AIMS/MBE. http://www.aimspress.com/journal/MBE 16(5): 4581–4593.

[29] Amit Doegara, Maitreyee Dutta, Gaurav Kumar. CNN based Image Forgery Detection using pre-trained AlexNet Model. Proceedings of International Conference on Computational Intelligence & IoT (ICCIIoT) 2018. https://www.ssrn.com/link/ijciiot-pip.html.

[30] 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.

[31] 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.

[32] 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.

[33] Marra, Francesco & Gragnaniello, Diego & Verdoliva, Luisa & Poggi, Giovanni. A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection, 2019.