Journal of Biological Engineering Research and Review, 2021; 8(2): 162-168
ISSN: 2349-3232 Online
Available online at www.biologicalengineering.in/Archive

Research Article

Forged Image Identification with Digital Image Forensic Tools

Satyendra Singh and Rajesh Kumar*

Departments of Electronics and Communication, JK Institute of Applied Physics and Technology, University Of Allahabad, Prayagraj, India

***Corresponding author. E-mail:** rajeshkumariitbhu@gmail.com (**Rajesh K**)

ARTICLE INFO:

Article History:
Received: 23/06/2021
Revised: 19/10/2021
Accepted: 11/11/2021
Published: 31/12/2021

Keywords:
Photo forensic; Fake image; Copy move forgery; DCT; Digital image; Forensic tools.

Citation: Singh S, Kumar R. Forged Image Identification with Digital Image Forensic Tools. Journal of Biological Engineering Research and Review. 2021, 8(2): 162-168.

Abstract: - Recent digital photography has shown rapid growth over the past few years, the use of digital image has become an important aspect of our daily life, such as magazines, newspapers, courtroom, social media, news channel etc. Nowadays, image manipulation is easy, due to availability of powerful photo editing application software like Adobe Photoshop and availability of cheap camera enabled mobile devices. And possible to add or remove new features from an image without leaving an important clue or trace. In this paper, we focus on the detection of copy move digital image forgery, it is one of the most common types of photo forgery techniques and compare with existing method. We mostly utilize two types of methods to identify copy-move forgery: block-based and key point-based. In block-based approach to identify tampered images, block features are extracted and compared. In this method, we used discrete cosine transform (DCT) algorithm for detection of copy move forgery detection. We are discussing about an important image forensics and image authentication tools. The digital image forensics tools have been designed to detect the origin of a digital image or if the content is real or changed without having any prior knowledge of the image under investigation. The goal of this study is to give a complete overview of the current state of the photo forensics.

INTRODUCTION

In this era of digitalization with emerging technology image has an importance in our daily life. Nowadays the scenario of communication totally changed. The communication with each other has changed after the decade of mid 90's. In present days, image capturing is easy for us with digital camera and smartphone. Image is used for visual communication on social media such as Twitter, Facebook, and Instagram etc. These social media platforms provide quick image and video sharing facilities for user with less operational knowledge. Mostly social network user share pictures over the internet. Due to the widely use of social network the spreading of misleading content in the form of fake images and videos. Spreading of fake image is faster in social media rather than mainstream media [1]. Developing the new user-friendly technologies and advance image processing tools or image editing software have made it easy to be tampered image to make false propaganda for blackmailing. The identification or tracing clue of forged image with their naked eye is not easy for a person. Digital image is not accepted in court room without proper evidence or analysed by the forensic analysis. So, the reliability of the image has been questioned, because image forgery is increased in current days. Digital image forensics is a growing research area and play important role in multimedia security which aims for ensuring the authenticity and integrity of an image. Therefore, many researchers are attracted to developed new technologies and tools to the area of digital image forensics for fake image detection. Researcher are developing variety of digital image forensic techniques to determine authenticity and processing history of digital image. In Figure 1 show the example of copy move forgery (a) is original image and (b) is fake image.

Fig. 1: Image (a) is the original image and (b) fake image

When a digital camera captures a picture, it contains a large amount of information known as EXIF data to the image file. This data contains all the important camera settings, model number, and brand as well as GPS data if setting is on. If we

want to be seen EXIF data. Some websites and tools are available such as Exifdata.com, photo sharing site flicker show lots of data if available. Window and Mac also provide metadata if you right click on the file Explorer or Finder.

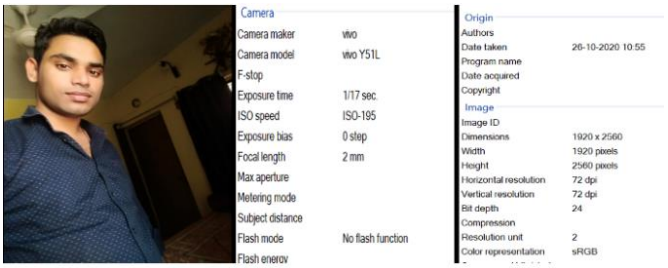

Fig. 2: Image with EXIF data

In above Figure II show EXIF data of an image which saved on my window system. We got some metadata related to this picture with the help of windows system.
A digital image generally copies of the data that we need to examine. There are some popular digital images forensic tool [2].

Forensic Tool Kit (FTK) Imager, this is available free for digital picture forensics. FTK Imager allows you to preview data on a device and create a forensically sound picture of the evidence without changing the device itself.
We discuss an important digital image authentication tool. There are some following tools available free for use.

1. Google reverse image search
2. Tin Eye
3. Reverse image search with Yandex
4. Reverse image search with Bing

Google image search is a well-known reverse image search tool. It allows you to rapidly get comparable results to the image you looked for.
We found the following results shown in Figure III, when we used Google's reverse image search function.

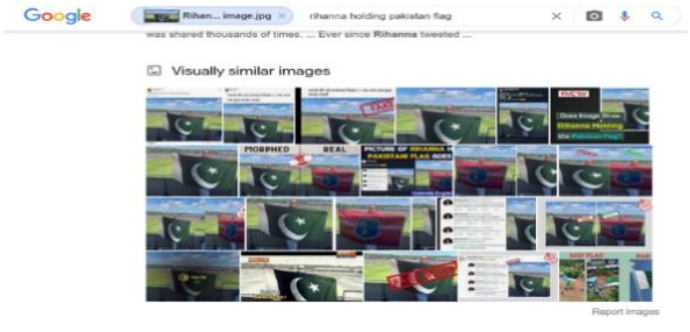

Fig. 3: Screenshot of Google reverse image search result

Tin Eye is a company, it provides image recognition and search techniques. Tin Eye is a good reverse image search tool, and which provide also good results. When we search reverse image on Tin Eye reverse image search tool, we received following results shown in Figure IV. Bing is a popular search engine, Microsoft created and designed it. And it is also used for reverse image search. Yandex is a reverse image search engine popular in the Russian Federation. It is generally giving good result outside the US and Western Europe.

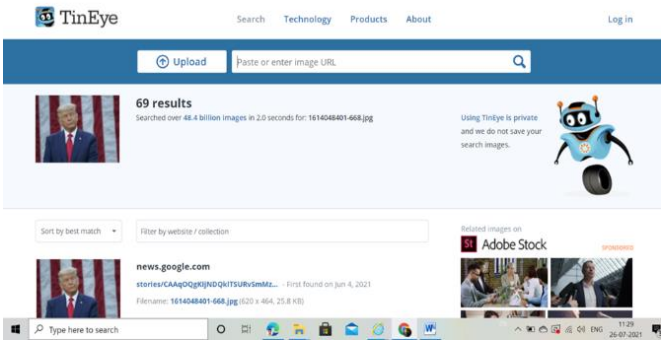

Fig. 4: Screenshot of Tin eye search result

LITERATURE REVIEW

Bayer B. et al. [3] have conducted an experiment. In this experiment the author has used a new approach, 'convolutional layer for universal image manipulation detection' based on deep learning techniques. The convolutional neural network architecture can automatically learn manipulation detection features from available training data. And this discussion remove problem, CNN is not capable to learn median filter detection features if image is directly fed to learn the input layer. This CNN model has classifiers binary and multiclass. The proposed model has good performance in binary classification to detect the tampered image region CNN differentiate between original and tampered image with at least 99.31% accuracy and this model achieve very high accuracy after performing thousands of iterations. Convolutional neural network model for multiclass classifier to detect multiple types of photo tampering. For example, gaussian blurring, median filtering, additive white gaussian noise etc. and result of this CNN classifier detect the four different types of forgery with 99.10% accuracy. So, this model is significant. Which is automatically detect multiple manipulation without changing its architecture or needing a human expert to identify detection features. And the average accuracy of this system is 99.10%.

Ding, F. et al. [4] in this study, author proposed a method based on deep learning technique & estimate the parameters of Gaussian filtering process images. The proposed system can ensure, the given image tampered or not in a quite short time. In this work solve the problem of estimating the parameters of gaussian filtered images. Using convolutional neural network (CNN). In this experiment seven convolutional layers are applied for better performance with accuracy 96.95%. And proposed method to be capable to process large scale of data quickly. Author also describes about if estimation accuracy major concern recommends seven layers model and if complete the estimation soon can be use six layers.

Marra, F. et al. [5] in this paper describe the method, 'detection of fake images on social networks generated by generative adversarial network (GAN)'. The proposed system is detecting image to image translation. This is very rare problem wherein images of some domains are mapped to corresponding images in another domain. In case of XceptionNet, it is well maintained by deep networks, which keeps working approximately well in the presence of training test mis matching. In the study of 36302 images

dataset and detection accuracy can be achieved 95% by both conventional and deep learning detectors.

Ouyang, J. [6] in this work, author proposed a model based on deep learning approaches for detection of copy move forgery. This model is trained large database as ImageNet and some small training samples. The reason is that ImageNet training model has well performance. The proposed method is not robust to the copy move forgery detection of image in real scenario. Author analyzed that the proposed method is not perfect. And so, this study has further scope to applied convolutional neural network to copy move image forgery detection.

Alahmadi, A. et al. [7] in this experiment study copy move and splicing image forgery detection method based on 'local binary pattern (LBP) and discrete cosine transform (DCT)'. In this detection used an SVM classifier. And the proposed method validates that chroma channels are better for forgery detection. For evaluation using three types of datasets, CASIA TIDE v1.0, CASIA TIDE v2.0 and Columbia datasets and result of the method in these dataset gives approximate similar i.e., accuracies are 97%, 97.5% and 97.77% respectively.

Nataraj, L. et al [8] developed a system for detection of GAN generated fake images with the help of group of co-occurrence matrices and deep learning techniques. And the co-occurrence matrices are computed based on color channels of images then trained a model using deep learning-based CNN to differentiate original image and GAN generated image. The proposed system achieved more than 99% classification accuracy in both databases are accuracy of 99.71% on the cycleGAN and 99.37% on the starGAN dataset.

Hashmi, M. F. et al [9] in this experimental study author developed a method to detect digital image forgery. In this detection method using combination of Un-decimated Wavelet Transform and scale invariant feature transformation (SIFT) for copy move image forgery detection. In this system first DyWT is applied on a given image and partition it into four different parts LL, LH, HL, and HH and then applied SIFT for feature extraction of each parts of an image and then matching is obtained in between feature descriptor to analyzed that given image is fake or not. The developed system achieves better performance and robustness in comparison to other common copy move forgery detection technique.

Marra, F. et al. [10] in this paper, designed a system to detect digital image forgery using deep learning-based techniques. The technique is a full-image full resolution end to end trainable framework. And the proposed convolutional neural network (CNN) framework is better performed in all cases with respect to all reference method.
Yarlagadda, S. K. et al [11] in this study, author proposed a system for detection of satellite image forgery and localization with the help of deep learning approaches. The proposed system has been used generative adversarial network (GAN) and one class classifier for image forgery detection. And the proposed model used generative adversarial network to train the autoencoder for the satellite image forgery detection task.

Mahalakshmi, S. D. et al [12] in this study proposed an image authentication technique & detect digital image manipulation. The basic image manipulation are involved such types of forgeries as copy move forgery, region duplication forgery, image splicing etc. in this paper detect some areas that is done in forged image such as contrast enhancement, histogram equalization and resampling (rotation, rescaling) and proposed method is tested in VSC-SIPI database and achieved accuracies in local rotation 96.3%, local rescaling 97.6%, local contrast enhancement 98.3 % and local histogram equalization 99.3%. In this experiment the resampling detection algorithms fail when JPEG compression is performed.

In the Table I show comparative literature of many papers discuss about an image forgery technique, detection domain and measurement accuracy.

Table 1: Comparative studies of various digital image forgery detection techniques

SN	paper	Techniques	Detection domain	Accuracy
1	Splicing Image forgery detection based on DCT and local binary pattern [13].	Local binary pattern (LBP) And discrete cosine transforms	Image splicing detection	Accuracy is 97%
3	Weakly-supervised domain adaptation for forgery detection [14].	Naive classification approach based on CNN	Manipulation detection	Accuracy is 95%
4	Copy moves forgery detection using DWT and SIFT features [15].	Discrete wavelet transforms	Copy move forgery	Accuracy is 94%
5	Splicing image forgery detection using textural features based on the gray level co-occurrence matrices [16].	Textural features based on the gray level co-occurrence (TF-GLCM)	Splicing detection	CASIA v1.0with accuracy is 98.54% & CASIA v2.0 with accuracy is 97.73%
6	Image region forgery detection, a deep learning approach [17].	Two stage deep learning approach	Region detection in multi format image	Accuracy of proposed method is 91.09%
7	Buster net detection copy move forgery with source target localization [18].	Deep learning technique	Copy move forgery	Accuracy is 78%

8	Deep learning local descriptor for image splicing detection and localization [19].	Deep learning-based CNN	Image splicing detection	Accuracy is 97.50%
9	Image splicing detection through illumination inconsistencies [20].	High representation power of illuminant maps and CNN	Image splicing	Classification accuracy is 96%
10	Detection fake image on social media using machine learning [21].	Deep learning-based CNN	Any threat and forged image	Accuracy is 97%
11	Image forgery detection a low computation-cost and effective data driven model [22].	Deep learning	Feature detection	Accuracy is 98.11%
12	Image splicing forgery detection based on improved LBP and k-nearest neighbours' algorithm [23].	Local binary pattern & DCT	Image splicing forgery	Accuracy of CASIA TIDE v1.0, CASIA v2.0 are 98% and 96% respectively
13	Detection of image forgery using information standard method with SVM [24].	SVM classifier	Feature extraction of an image	Accuracy is 98.5%
14	Copy moves and splicing forgery detection using CNN and semantic segmentation [25].	Deep convolution Neural network and semantic segmentation	Copy-move forgery and splicing	Accuracy is above 98%
15	Automated image splicing detection using deep CNN-learned features & ANN based classifier [26].	Deep learning-based CNN and ANN classifier	Image splicing forgery	Dataset CASIA v2.0 with accuracy more than 96%
16	Fake face detection via adaptive manipulation traces extraction network [27].	Deep learning based an adaptive manipulation traces extraction network	Fake face detection	Average accuracy of AMTEN is 98.52%
17	A deep learning-based method for image splicing detection [28].	Deep learning	Image splicing	CUISDE dataset average accuracy is 97.24%

METHODS

We proposed a method to detect copy move image forgery using discrete cosine transformation (DCT), The Discrete Cosine Transform (DCT) is a Fourier-related transform that describes a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. It is similar to the Discrete Fourier Transform (DFT) but uses only real numbers. DCT represent an image as a series of sinusoids with different magnitudes and frequencies. The significant energy compaction and decorrelation properties of DCT make it a popular image processing technique. The N×N cosine matrix is defined as

$$C = \{c(k, n)\}$$

$$C(k, n) = \begin{cases} \frac{1}{\sqrt{N}} & k = 0,\ 0 \le n < N-1 \\ \frac{\sqrt{2}}{N} cos \frac{\pi(2n+1)}{2n}, & 1 \le k \le N-1 \\ & 0 \le n \le N-1 \end{cases} \quad (1)$$

Where k is row and n column, in equation (1) define N× N DCT matrix. In the DCT experiment set the parameters quantization factor, Euclidean distance similarity threshold, Euclidean distance between pixel threshold and block size.

The quantization steps are determined during forgery detection using a user-specified parameter Q, which sets the quantization steps for DCT transform coefficients.

A color input image I with a size of H× W is converted to a grey scale image in the first stage using

I = 0.229R + 0.587G + 0.114B ……. (2)

Each block is represented by Brc, where r and c are the row and column starting points, respectively. In equation (2) R, G, and B represents the three-color components of RGB color model. RGB input image to reduce the computation. In the next step split a grey scale image into overlapping blocks b× b then DCT coefficient characteristics are extracted from each block. Apply DCT to each block and reformat the quantized coefficient matrix into a row vector by zigzagging the DCT coefficients. Then similarity between blocks is analyzed after vectors are sorted lexicographically in ascending order.

Finally find the correct blocks and output them or the resulted image. And measure performance of DCT precision, recall and accuracy though comparison of similarity index.

Algorithm structure

Following figure V shows the algorithm structure of proposed method. In this structure describe the step-by-step flow of code of proposed method.

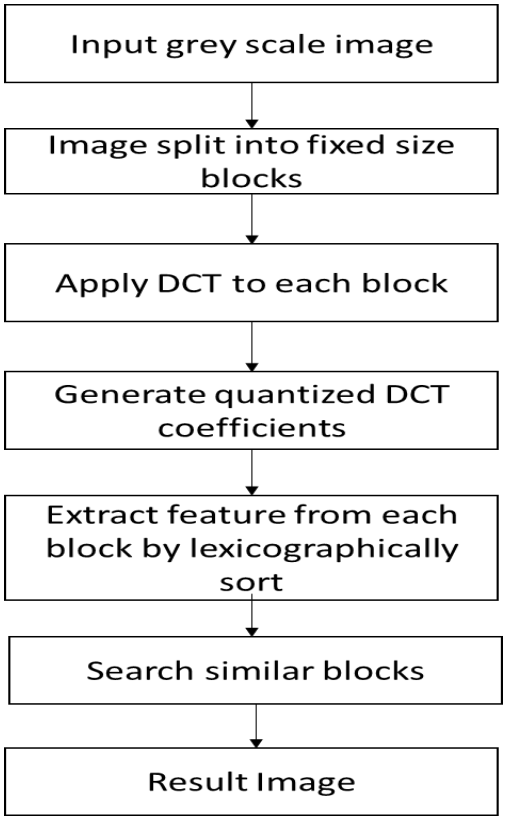

Fig. 5: Algorithm Framework

Performance measurement

The parameters for measuring image level are as follows [29]:

Tp – True positive – tampered image predicted as original.
Tn – True negative – original image predicted as original.
Fp – False positive – original image predicted as tampered.
Fn – False negative – forged image predicted as original.
Precision: - probability that an identified forgery is truly a forgery, computed as

$$P = \frac{Tp}{Tp+Fp} \quad \ldots\ldots\ldots\ldots\ldots \quad (3)$$

Recall: - 'r' denotes the probability that a forged image is detected, computed as

$$P = \frac{Tp}{Tp+Fn} \quad \ldots\ldots\ldots\ldots\ldots (4)$$

Accuracy: - the ability of the method to measure the accurate value is known as accuracy

$$\text{Accuracy} = \frac{Tp+Tp}{TP+Tn+Fp+Fn} \quad \ldots\ldots\ldots\ldots (5)$$

Equations (3), (4) and (5) are formula to calculate precision, recall and accuracy respectively.

EXPERIMENTAL SETUP AND RESULTS

The experiment is performed on a plate form with window 10 operating system, Intel i5 1.80 GHz processor, 8GB RAM and python 3.8.3. The original image and mask image are tested and image in PNG format. The experimental result proposed in this section and screenshot of result shown in below Figure VI calculate accuracy is 97%, precision 99 % and recall 95% and exist approach proposed by Christlein [30]. The proposed method will be compared to the existing method in terms of accuracy, recall and precision. In the existing method image is divided into 8× 8 fixed sizes of blocks. But in this experiment image is divided into 6×6 fixed sizes of blocks. So, the proposed method accuracy is improved as compare to existing method. Figure VI is shown experimental result.

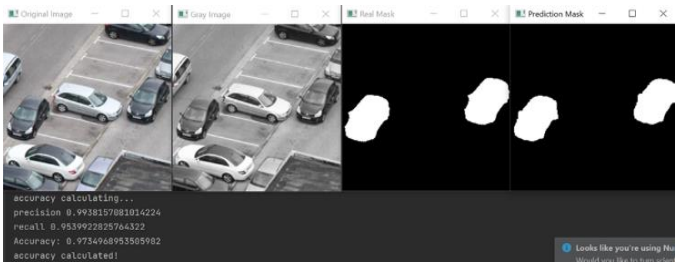

Fig. 6: Experimental Result

Table II shows the calculated results of performance measurement in percentage of proposed method, and comparison with calculated performance of existing method.

Method	Accuracy	Precision	Recall
Christlein, V., et al [30]	89.34	78.69	100
Proposed	97	99	95

DISCUSSION

In the proposed experimental work, copy move forgery has been detected. The proposed method demonstrates the better results with good accuracy in comparison to other existing approaches. The above Table II shows the results of proposed method and existing method. The performance of proposed method in terms of accuracy, precision and recall are 97%, 99%, and 95% respectively. The overall performance of proposed method betters in comparison to existing methods.

CONCLUSION

In this paper, digital image authentication tools and techniques has been implemented to detection the copy move forgery using DCT. The discrete cosine transformation (DCT) is applied to detect copy move image forgery and compared with existing literature. Experimental results show that the accuracy is 97%, precision 99% and recall 95%. From above results and analysis, we are in position to say that this method provides better results as compare to existing method.

REFERENCES

1. Sahoo, S. R., & Gupta, B. B. (2021). Multiple features-based approach for automatic fake news detection on social networks using deep learning. Applied Soft Computing, 100,106983.
2. Olson, E., & Shashidhar, N. (2016). Low Budget Forensic Drive Imaging Using Arm Based Single Board Computers. Journal of Digital Forensics, Security and Law, 11(1), 3.
3. Bayar, B., & Stamm, M. C. (2016, June). 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 (pp. 5-10).).
4. Ding, F., Shi, Y., Zhu, G., & Shi, Y. Q. (2020). Real-time estimation for the parameters of Gaussian filtering via deep learning. Journal of Real-Time Image Processing, 17(1), 17-27.
5. Marra, F., Gragnaniello, D., Cozzolino, D., & Verdoliva, L. (2018, April). Detection of gan-generated fake images over social networks. In 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) (pp. 384-389). IEEE.
6. Ouyang, J., Liu, Y., & Liao, M. (2017, October). Copy-move forgery detection based on deep learning. In 2017 10th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI) (pp. 1-5). IEEE.
7. Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G., & Mathkour, H. (2017). Passive detection of image forgery using DCT and local binary pattern. Signal, Image and Video Processing, 11(1), 81-88.
8. Nataraj, L., Mohammed, T. M., Manjunath, B. S., Chandrasekaran, S., Flenner, A., Bappy, J. H., & Roy-Chowdhury, A. K. (2019). Detecting GAN generated fake images using co-occurrence matrices. Electronic Imaging, 2019(5), 532-1.
9. Hashmi, M. F., Anand, V., & Keskar, A. G. (2014). Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform. Aasri Procedia, 9, 84-91.
10. Marra, F., Gragnaniello, D., Verdoliva, L., & Poggi, G. (2020). A full-image full-resolution end-to-end-trainable CNN framework for image forgery detection. IEEE Access, 8, 133488-133502.
11. Yarlagadda, S. K., Güera, D., Bestagini, P., Maggie Zhu, F., Tubaro, S., & Delp, E. J. (2018). Satellite image forgery detection and localization using gan and one-class classifier. Electronic Imaging, 2018(7), 214-1.
12. Mahalakshmi, S. D., Vijayalakshmi, K., & Priyadharsini, S. (2012). Digital image forgery detection and estimation by exploring basic image manipulations. Digital Investigation, 8(3-4), 215-225.
13. Alahmadi, A. A., Hussain, M., Aboalsamh, H., Muhammad, G., & Bebis, G. (2013, December). Splicing image forgery detection based on DCT and Local Binary Pattern. In 2013 IEEE Global Conference on Signal and Information Processing (pp. 253-256). IEEE.
14. Cozzolino, D., Thies, J., Rössler, A., Riess, C., Nießner, M., & Verdoliva, L. (2018). Forensictransfer: Weakly-supervised domain adaptation for forgery detection. arXiv preprint arXiv:1812.02510.
15. Hashmi, M. F., Hambarde, A. R., & Keskar, A. G. (2013, December). Copy move forgery detection using DWT and SIFT features. In 2013 13th International conference on intellient systems design and applications (pp. 188-193). IEEE.
16. Shen, X., Shi, Z., & Chen, H. (2017). Splicing image forgery detection using textural features based on the grey level co-occurrence matrices. IET Image Processing, 11(1), 44-53.
17. Zhang, Y., Goh, J., Win, L. L., & Thing, V. L. (2016). Image Region Forgery Detection: A Deep Learning Approach. SG-CRC, 2016, 1-11.
18. Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018). Busternet: Detecting copy-move image forgery with source/target localization. In Proceedings of the European Conference on Computer Vision (ECCV) (pp. 168-184).
19. Rao, Y., Ni, J., & Zhao, H. (2020). Deep learning local descriptor for image splicing detection and localization. IEEE Access, 8, 25611-25625.
20. Pomari, T., Ruppert, G., Rezende, E., Rocha, A., & Carvalho, T. (2018, October). Image splicing detection through illumination inconsistencies and deep learning. In 2018 25th IEEE International Conference on Image Processing (ICIP) (pp. 3788-3792). IEEE.
21. AlShariah, N. M., Khader, A., & Saudagar, J. Detecting Fake Images on Social Media using Machine Learning.
22. Le-Tien, T., Phan-Xuan, H., Nguyen-Chinh, T., & Do-Tieu, T. (2019). Image forgery detection: A low computational-cost and effective data-driven model. International Journal of Machine Learning and Computing, 9(2).
23. Hakimi, F., Hariri, M., & Azad, I. (2015). Image-splicing forgery detection based on improved lbp and k-nearest neighbors' algorithm. Electronics Information & Planning, 3(0304-9876), 7.
24. Mohammed, A. H., Badr, D. H., & Ali, F. (2021, March). Detection of Image Forgery Using Information Standard Method With SVM. In Journal of Physics: Conference Series (Vol. 1818, No. 1, p. 012212). IOP Publishing.
25. Jindal, N. (2021). Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation. Multimedia Tools and Applications, 80(3), 3571-3599.
26. Nath, S., & Naskar, R. (2021). Automated image splicing detection using deep CNN-learned features and ANN-based classifier. Signal, Image and Video Processing, 1-8.
27. Guo, Z., Yang, G., Chen, J., & Sun, X. (2021). Fake face detection via adaptive manipulation traces extraction network. Computer Vision and Image Understanding, 204, 103170.
28. Meena, K. B., & Tyagi, V. (2021, January). A Deep Learning based Method for Image Splicing Detection. In Journal of Physics: Conference Series (Vol. 1714, No. 1, p. 012038). IOP Publishing.
29. Suresh, G., & Rao, C. S. (2019). Copy-move forgery detection system through fused color and texture features using firefly algorithm. Int. J. Recent Technol. Eng., 8, 2559-2567.
30. Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. IEEE

Transactions on information forensics and security, 7(6), 1841-1854.

About Authors

Mr. Satyendra Singh received the B.Sc. and M.Sc. degree in computer science from University of Allahabad, Prayagraj, INDIA. He is currently a Ph.D. research scholar at Department of Electronics and Communication (JK Institute of Applied Physics and Technology), University of Allahabad. He has been working on Computer vision and Image Processing. His research interests include Digital Image Forensics, Machine Learning and Deep learning.

Dr. Rajesh Kumar is working as an Assistant professor in the Department of Electronics and Communication at the University of Allahabad, Prayagraj, India. He received the BE degree in Computer Science and Engineering from faculty of Engineering, HNB Garhwal University, Srinagar, U.K., India, MTech degree in software engineering from Motilal Nehru National Institute of Technology, Allahabad, India and PhD degree in Computer Engineering from Indian Institute of Technology (BHU), Varanasi, India. He has around 12 years of teaching and 8 years of research experience. His research interests include Computer Vision, Image Processing and Medical Image Analys.