International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 07 | July 2022 www.irjet.net p-ISSN: 2395-0072

Image Forgery Detection Methods- A Review

Sonali Ankolikar[1], Samiksha Agrawal[2], Rupal Mohanty[3]

[1]Student, School of Electronics and Communications Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune-411038, Maharashtra, India
[2]Student, School of Electronics and Communications Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune-411038, Maharashtra, India
[3]Student, School of Computer Science and Engineering, Dr. Vishwanath Karad MIT World Peace University, Pune-411038, Maharashtra, India

---***---

Abstract - *In today's world, we are constantly surrounded by the exploitation of image manipulation techniques and the circulation of forged images on the internet. With this, the need for regulation methods and image forgery detection techniques has risen and it is evident that to understand different detection methods. In this paper, we review the various methods by which images can be manipulated and provide a comparative analysis of the different techniques to detect image forgery in a comprehensive manner with respect to all the literature available from the past decade. This comparison has been done to understand which methods prove fruitful under respective circumstances and to ensure that future implementations in this area of research are able to create an independent model which will successfully identify the forgery in an image without human intervention.*

***Key Words*: Forgery, detection, image manipulation, human intervention, image forensics**

1.INTRODUCTION

Image manipulation is the application of using various techniques for altering images in order to create a deception. The modern world around generating diverse art has created a huge deposit of fake, doctored images. Digital image forensics has been developed in order to provide tools for blind investigations. It originally stems from the existing domains of research falling under the umbrella of image forensics. Moreover, it exploits the properties of image processing and analysis tools to understand the processing of the data and recovery of information from the images. This underscores our efforts to understand which image detection techniques are effective, accurate, and provide quick results. We believe it is key to restoring the integrity of images that are not generated by taken from their authentic sources.

As the act of faking images is not new to the modern 'generation' (cultural reference-Generation Z), deep fakes and image manipulation techniques continue to display powerful abilities to generate visual and audio content with the help of artificial intelligence and machine learning despite the curbing measures implemented by governments and institutions across the world. The main architecture of these image manipulation techniques is based on GAN- Generative Adversarial Network. There are majorly 2 digital forensics methods that are largely followed in the industry. The first method includes methods that attempt to understand the image by performing a ballistic analysis of it and creating an understanding of what kind of device was used / not used to capture it. The second method consists of the method for exposing traces of tampering or semantic manipulation by calculating the inconsistencies in natural image forgery techniques.

2. METHODOLOGY

Types of manipulation can be generally classified into 3 categories:

- Copy move mechanism
- Image forgery using splicing
- Retouching

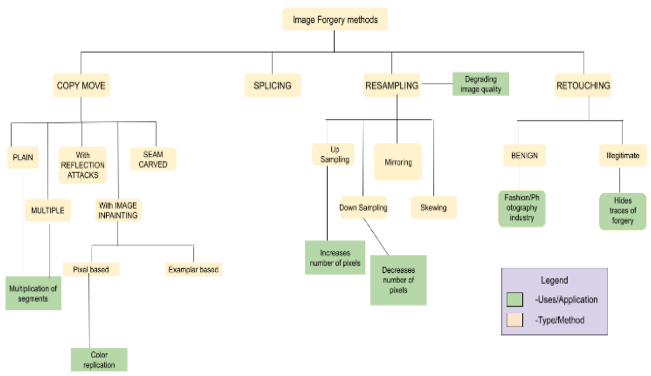

Fig -1: Tree diagram of the methods implemented in image manipulation

Throughout the domain, there are an immense number of methodologies we observed. Doctoring an image can have a lasting effect on the image and the subject. It can create a false identity and generate false beauty standards. Studies suggest that one in every 5 images is doctored or manipulated. This raises the concern for the need for detection of manipulation because the data generated or images generated in today's world are the heritage of the coming generations. The first methodology addressed is a CNN universal forgery detection method. It consists of a pre-trained model and is an active method of detection used. It does not require human interaction to create the detector.

The term "convolutional neural network" indicates that the network employs a mathematical operation called convolution. Convolutional networks are a specialized type of neural network that uses convolution in place of general matrix multiplication in at least one of their layers. CNNs are regularized versions of multilayer perceptrons. Multilayer perceptrons usually mean fully connected networks, that is, each neuron in one layer is connected to all neurons in the next layer. The "full connectivity" of these networks makes them prone to overfitting data.

Typical ways of regularization or preventing overfitting, include: penalizing parameters during training (such as weight decay) or trimming connectivity (skipped connections, dropout, etc.) CNN's take a different approach towards regularization: they take advantage of the hierarchical pattern in data and assemble patterns of increasing complexity using smaller and simpler patterns embossed in their filters. Therefore, on a scale of connectivity and complexity, CNNs are on the lower extremity. CNNs use relatively little pre-processing compared to other image classification algorithms. This means that the network learns to optimize the filters (or kernels) through automated learning, whereas in traditional algorithms these filters are hand-engineered.

This independence from prior knowledge and human intervention in feature extraction is a significant advantage. Convolutional networks may include local and/or global pooling layers and traditional convolutional ones. Pooling layers reduce the dimensions of data by combining the outputs of neuron clusters at one layer into a single neuron in the next layer. Local pooling combines small clusters, and tiling sizes such as 2 x 2 are commonly used. Global pooling acts on all the neurons of the feature map. Fully connected layers connect every neuron in one layer to every neuron in another layer. It is the same as a traditional multi-layer perceptron neural network (MLP). The flattened matrix goes through a fully connected layer to classify the images. One more dependency observed was that a CNN with more kernels yields better results, the use of more kernels requires more time for training.

Table -1: Comparison of methods with respect to corresponding sources of literature

Title	Description	Technique/Method	Accuracy	Citation
Constrained R-CNN: A General Image Manipulation Detection model, Chao Yang, Huizhou Li, Fangting Lin, Bin Jiang, Hao Zhao	In this literature, they have worked on restrained CNN and used a learnable manipulation feature extractor to create a unified feature representation of various content from the image data. Moreover, it explains how a coarse to simulate a fine forensic process in the real world	1. Achieves manipulation techniques classification and manipulated region segmentation simultaneously. 2 A single-stream learnable manipulation feature extractor. 3. An attention regional proposal network (RPN-A)	-	4
Automated image splicing detection using deep CNN-learned features, Souradip Nath, Ruchira Naskar	In this paper, we propose an automated image splicing detection scheme using deep CNN-learned features and ANN-based classifier. The proposed approach involves two main steps: (A)feature engineering and (B) classification	A blind image splicing detection technique using a deep convolutional residual network architecture as a backbone, followed by a fully connected classifier network, that classifies between authentic and spliced images.	96%	11
A Deep Learning based Method for Image Splicing Detection, Kunj Bihari Meena and Vipin Tyagi 2021 J. Phys.: Conf. Ser. 1714 012038	This paper explains the implementation of a deep learning-based method to detect image splicing in the images. The input image is preprocessed using a technique called 'Noiseprint' to get the noise residual by suppressing the image content.	The architecture of the proposed method consists of 3 main steps : 1. Obtaining noise residual map using the Noiseprint 2. Extracting features using ResNet-50 3. Feature classification using support vector machine	97.24%	12

	Second, the popular ResNet-50 network is used as a feature extractor			
K. M. Hosny, A. M. Mortda, M. M. Fouda, and N. A. Lashin, An Efficient CNN Model to Detect Copy-Move Image Forgery	Copy move forgery detection using a method of a CNN based model for image forgery detection.	A deep CMF method along with CNN. A feature extraction layer consists of 3 convolution layers followed by a max-pooling layer and a full connection layer at the ends.	100%	44
JPEG Compression without CNN techniques:				
Learning Rich Features for Image Manipulation Detection, Zhou, Peng & Han, Xintong & Morariu, Vlad & Davis, Larry	This literature explains a faster R-CNN network and trained model to detect the tampered regions in a doctored image end to end.	RGB stream-extracts feature from the RGB image input to find tampering artifacts like strong contrast difference, unnatural tampered boundaries, etc. stream 2-Tends to leverage the noise features extracted from a steganalysis rich model filter layer to discover the noise inconsistency	93%	6
Double JPEG compression forensics based on a convolutional neural network, Wang, Qing, and Rong Zhang	In this literature, it aims at performing preprocessing on DCT coefficients and histograms which are further extracted as input and sent through a CNN for the features to be learned. Later its job is to distinguish the double JPEG compression forgeries and	• Uses two convolutional layers, kernel size to 3 × 1, • Using different feature dimensions-71% to 79.4%; • Using different training set sizes-50% to 79.1%; • Uses different numbers of kernels-71.6% to 79.6%;	70 % to 80%	7
	achieve localisations.			
Rao, Yuan, and Jiangqun Ni. "Self-supervised domain adaptation for forgery localization of JPEG compressed images."	This literature proposes a self-supervised domain adaptation network and a compression approximation network is proposed for JPEG-resistant image forgery localization.	Contains a backbone network.	-	41
Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression Vega, Esteban Alejandro Armas; Fernandez, Edgar Gonzalez; Orozco, Ana Lucila Sandoval; Villalba, Luis Javier Garcia	This paper proposes a digital image authentication method based on the quadratic mean error of color filter array interpolation pattern estimated from the analyzed image.	Makes use of Error level analysis along with the color filter analysis to figure out the interpolation pattern of the color filter.	73.30%	42
Bo Liu, Chi-Man Pun, Xiao-Chen Yuan, "Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies",	Carries out image forgery detection by using a blockwise specialized descriptor and then a forehand image quality assessment procedure is implemented.	Block artificial grids followed by mapping after which the feature generation for 8x8 blocks are generated. Noise feature extraction is later carried out using SLIC segmentation.	Variable from 80 % to 100% w.r.t the JPEG compression ratio.	43
Transform Techniques:				

Research on Copy-Move Image Forgery Detection Using Features of Discrete Polar Complex Exponential Transform, Yanfen Gan & Junliu Zhong	It covers an unused strategy based on the Polar exponential change which is proposed in order to address various issues of the image features.	Template is formulated such that 1 pixel passed at a time, lexicographic is used for invariance features, judge, detect and locate to forgery region of the image	65%	8
Image splicing detection based on Markov features in QDCT domain, Ce Lia, Qiang Mab, Limei Xiaob, Ming Lib, Aihua Zhang	The proposed approach in this literature is that the model is based on Markov features of the image and their values in the QDCT domain are introduced and observed.	Applying 8×8 block QDCT on the original image pixel array and the corresponding QDCT coefficient array is obtained. Secondly, rounding the QDCT coefficients to integer and taking the absolute value. Thirdly, calculate the horizontal, vertical, main diagonal, and minor diagonal intra-block difference 2-D arrays.	93%	9
DCT-domain Deep Convolutional Neural Networks for Multiple JPEG Compression Classification, Vinay Verma, Nikita Agarwal, and Nitin Khanna	This literature focuses on the process of differentiating between images based on the number of compressions the features of the image have undergone by extracting histogram-based features and then feeds them into a CNN.	CNN architectures such as AlexNet, VGGNet, GoogLeNet, and ResNet with a filter of size 3 × 1 (kernel size), the network has four convolutional layers followed by three fully-connected layers	86%	10
Double JPEG Compression Detection Based on Noise-Free DCT Coefficients Mixture Histogram Model, Zhu, Nan, Junge Shen, and Xiaotong Niu. 2019.	This paper talked about an improved double JPEG compression detection method based on noise-free DCT (Discrete Cosine Transform) coefficients mixture histogram model.	1. Method based on noise-free DCT coefficients mixture histogram model 2. By eliminating the quantization noise, 3. Resort to the split noise filtering algorithm 4. 100 uncompressed images with size 1024 × 1024 5. Treated double and single JPEG compressed pixels as positive and negative samples, respectively	Varying between 50 to 100%	13
Hegazi, Aya; Taha, Ahmed; Selim, Mazen M. (2019). An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal.	In this paper, a keypoint-based copy-move forgery detection is proposed. The proposed method which is based on density-based clustering and Guaranteed Outlier Removal algorithm.	In this paper, the model implements CLAHE for preprocessing and image feature extraction using SIFT and then moves on to match suing density based clustering.	100%	17
Hayat, Khizar; Qazi, Tanzeela (2017). Forgery detection in digital images via discrete wavelet and discrete cosine transforms.	A forgery detection method which works on the transform domains technique relying on DCT and DWT for copy/move forgery	Reduces the features using DWT and then works by applying DCT on the blocks (reduced features of the image). These are further lexicographically reduced and correlated.	73.62%	19

Mahmood, Toqeer; Mehmood, Zahid; Shah, Mohsin; Saba, Tanzila (2018). A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform.	This literature proposes the robust technique using CMF detection and localisation in digital images.	This technique is implemented using a SWT based on features which is used for exposing forgeries in the images	Varying case wise	20
Gani, Gulnawaz; Qadir, Fasel (2020). A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata.	A robust method for detecting copy move forgery under different forgery attacks using DCT and cellular automata	It uses DCT to extract features from each block then the Cellular Automata is employed to construct feature vectors based on the sign information of the DCT coefficients. Then the feature vectors are matched using the kd-tree based nearest-neighbor searching method to find the duplicated areas in the image.	Varies case wise but maintains its accuracy between 70% to 90%	21

Table -2: Comparison of methods with respect to corresponding Advantages and Future Scope

Title	Advantages	Future Scope	Citation No.
Using CNN related methods			
A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer, Belhassen Bayar, Matthew C. Stamm	Uses a deep learning model, improved accuracy, introduced a new convolution layer, reduction in overfitting of the model.	Time complexity increases, and the lengthy process	[1]
Image Manipulation Detection using Convolutional Neural Network, Kim, D.-H & Lee, H.-Y.	Uses modified images generated using median filter processing, Gaussian Filtering, and blurring, Additive white Gaussian noise addition with image resizing.	It can be applied for the detection of more manipulation techniques if a better model is established in later studies. In addition, it will be possible to apply it to various multimedia as well as image in further research	[2]
Developing an Image Manipulation Detection Algorithm Based on Edge Detection and Faster R-CNN, Xiaoyan Wei, Yirong Wu, Fangmin Dong, Jun Zhang &Shuifa Sun	Instead of using a max-pooling approach, the Bilinear interpolation method is used to obtain the RoI region. A regional Proposal Network is used to locate the forgery locations.	Multiple features of tampered images could be fused to find more tampering clues and improve image manipulation detection performance.	[3]
Constrained R-CNN: A General Image Manipulation Detection model, Chao Yang, Huizhou Li, Fangting Lin, Bin Jiang, Hao Zhao	Can capture manipulation clues directly from data without any handcrafted component.	Limited to manipulation classification and localization.	[4]
Automated image splicing detection using deep CNN-learned features and ANN-based classifier, Souradip Nath & Ruchira Naskar	With the experimental results , it is demonstrated that the performance of the proposed model is superior to that of the state of the art.	This model can only detect whether an image is spliced or not but does not involve the localization of sliced regions within such an image. In real-life cases, this is of utmost importance.	[11]
A Deep Learning based Method for Image Splicing Detection, Kunj Bihari Meena and Vipin Tyagi 2021 J. Phys.: Conf. Ser. 1714 012038	The usage of the nose printing method enables the model to highlight the tampered parts of the image with much higher accuracy.	It doesn't tell us any information about the spliced region and avoids heading into the analytics of the image.	[12]

K. M. Hosny, A. M. Mortda, M. M. Fouda, and N. A. Lashin, An Efficient CNN Model to Detect Copy-Move Image Forgery	Obtains an accuracy of 100% and is quick and accurate.	This model needs to be trained first and then tested.	[44]
JPEG Compression without CNN techniques:			
Learning Rich Features for Image Manipulation Detection, Zhou, Peng & Han, Xintong & Morariu, Vlad & Davis, Larry	Fusion of features from the two streams through a bilinear pooling layer to further incorporate spatial co-occurrence of these two modalities	Can be infused in a much better manner with better JPEG compression techniques.	[6]
Double JPEG compression forensics based on a convolutional neural network, Wang, Qing, and Rong Zhang	Achieves localization automatically and has a better performance only on certain QF values which still haven't been automated.	The computational complexity of the CNN is considerably high, thus generating a trade-off between the localization accuracy cap-ability and the computational effort required	[7]
Rao, Yuan, and Jiangqun Ni. "Self-supervised domain adaptation for forgery localization of JPEG compressed images."	Performs better in cases where jpeg images are compressed with unknown QFs, therefore, giving the proposed method a superior generalization ability.	The QF factors considered in the compression of JPEGs are extreme and may not be applicable for regular real-world cases.	[41]
Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression Vega, Esteban Alejandro Armas; Fernandez, Edgar Gonzalez; Orozco, Ana Lucila Sandoval; Villalba, Luis Javier Garcia	Since the proposed model doesn't just consider features, it has a better chance at localisation of the part of the image that has been forged because it can compare the contents of the original image from the manipulated parts.	The model successfully works only for images with dimensions of 700 x 700 pixels or greater. Hence more work for the proposed method to be able to work on the smaller images is yet to be done.	[42]
Bo Liu, Chi-Man Pun, Xiao-Chen Yuan, "Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies"	Has a simulation-based approach hence is able to simulate and counter a real splicing attack due to its implementation using a factor that calculates the coefficient using the image equality. It is highly applicable to highly compressed and high-quality images.	Its accuracy is dependent on the JPEG compression ratio.	[43]
Transform Techniques:			
Research on Copy-Move Image Forgery Detection Using Features of Discrete Polar Complex Exponential Transform, Yanfen Gan & Junliu Zhong	Reduces rounding errors of the transform from the Polar coordinate system to the Cartesian coordinate system, a new transformation method is presented and discussed in detail at the same time.	Relies heavily on complex algorithms hence the time needed is a lot. Lexicographic sorting does not ease the complexity but rather increases it.	[8]
Image splicing detection based on Markov features in the QDCT domain, Ce Lia, Qiang Mab, Limei Xiaob, Ming Lib, and Aihua Zhang	Works better on the dataset used than other models with the blind detection model on color images.	Does not possess theoretical value but is more inclined toward practical value.	[9]

DCT-domain Deep Convolutional Neural Networks for Multiple JPEG Compression Classification, Vinay Verma, Nikita Agarwal, and Nitin Khanna	1. It directly utilizes JPEG bitstream and reduces any additional effect of performing DCT on the data fed to the CNN, outperforming the existing system for multiple JPEG compression classifications	Limitation of the proposed method is the requirement of the same compression chains in training and testing data.	[10]
Double JPEG Compression Detection Based on Noise-Free DCT Coefficients Mixture Histogram Model , Zhu, Nan, Junge Shen, and Xiaotong Niu. 2019.	Since for each DCT frequency, a posterior probability is obtained by solving the DCT coefficients mixture histogram with a simplified model it ensures a much smarter model.	The quantization noise is needed to be improved upon as it may result in false detection of false tampered regions.	[13]
Hegazi, Aya; Taha, Ahmed; Selim, Mazen M. (2019). An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal.	The method implemented gives a collective accuracy of 95.83 % since the SIFT is actively able to robustly detect the forgery in jpg compression and feature transform methods.	The choice of number of blocks will hamper the accuracy and performance of the model and affect the SIFT	[17]
Hayat, Khizar; Qazi, Tanzeela (2017). Forgery detection in digital images via discrete wavelet and discrete cosine transforms.	The mask multiplication based method with the melange of the DCT and DWT methods were crucial in creating a less false detection rate.It possesses viability for both splicing and copy move forgery methods	May underperform in the case of occlusion.	[19]
Mahmood, Toqeer; Mehmood, Zahid; Shah, Mohsin; Saba, Tanzila (2018). A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform.	Implementation pf SWT, DCT,and CMFD techniques makes it more robust and makes representation of features more diverse.	Post-processing operations make detection of CMF challenging.	[20]
Gani, Gulnawaz; Qadir, Fasel (2020). A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata.	Effective under robust methods and can detect in presence of noise and combined attacks.	Possesses unattractive time complexity.	[21]

3. RESEARCH GAP AND FUTURE SCOPE

The vast gaps in image manipulation detection techniques start with the continuously evolving methods of artificial intelligence and machine learning techniques to improve the quality of manipulated images and content. When it comes to identifying one unique reliable and accurate method for all possible images, many of the detection techniques fall short of data sets availability.

Even though all the highly specific methods are robust, one cannot deny the need for the presence of human intervention. This poses a gap in research. By considering the multiple features of the image (which is normally in RGB) song with its noise features, the RGB-N generates the correct classification for different tampering techniques which makes it genuinely robust. This method is largely applicable across various image manipulation techniques. However, in cases of JPEG compression, it is still to be accurately developed. Although many suggest using deep learning models as an approach to apply a generalized solution to the detection techniques it fails to come across in terms of the power of giving a good performance in several applications. At times of innocent manipulations i.e., those carried out by error of machine or quality deterioration (examples-unintended blurring/reduction in the files quality/compression etc.), method-specific models can sometimes identify it as a manipulation. Such cases must be considered in the datasets instead of having them identified. Ultimately, copyrighting proves most essential in providing proof of successful detection of fake images as well. With the copyright, original images can be recognized and safely stored from manipulation regardless of who has access to it

Challenges in image manipulation detection techniques include:

- Processing of Video includes many security issues (Watermarking, Encryption, and Steganography) using the different compression techniques.
- Video transmission over real wireless channels.
- Image enhancements based on Fusion techniques which is a very hot topic, especially for medical purposes.
- Deep learning and its wide applications in Signal processing.
- The Application of the Advanced Optimization techniques for solving the multi-variable problems in several digital signal processing problems.

Throughout the kinds of literature reviewed and studied, many challenges were observed over the span of all the various techniques and proposed methods. In cases where the features were being detected and scrutinized using the transformation techniques, although they were highly robust and powerful, they were seen to be susceptible to factors like additive white noise, the combination of attacks, time complexities, and precision. The dimensionality reduction-based methods tend to ignore the crucial data which results in a lack of robust results and accuracy in cases of geometric transformations. This made it difficult to identify how many features are exactly enough for transformation-based techniques since even though the accommodation of multiple features will increase the accuracy of the results of the model it will result in an unattractive time complexity which is not desirable for most of the time in case of forensics. Texture-based detection methods, since they function block wise, tend to also be sensitive to the scaling operations, rotation operations, and jpeg compressions.

4. CONCLUSIONS

Despite the rise in technologies to detect the forgery of media, it has become terribly difficult to differentiate between real and fake images even with the intervention of humans. Thus the symbiotic relationship between humans and A.I. are vast for application in the field of law enforcement and forensics. Through this review, we conducted comparative research on how successful a certain method would be in order to see what would be a more robust and accurate approach to any image regardless of the image manipulation method. With more research in the future, it could be possible to implement such a model.

REFERENCES

[1] Bayar, Belhassen, and Matthew 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, pp. 5-10. 2016.

[2] Kim, Dong-Hyun, and Hae-Yeoun Lee. "Image manipulation detection using convolutional neural network." International Journal of Applied Engineering Research 12, no. 21 (2017): 11640-11646.

[3] Wei, Xiaoyan, Yirong Wu, Fangmin Dong, Jun Zhang, and Shuifa Sun. "Developing an image manipulation detection algorithm based on edge detection and faster r-CNN." Symmetry 11, no. 10 (2019): 1223.

[4] Yang, Chao, Huizhou Li, Fangting Lin, Bin Jiang, and Hao Zhao. "Constrained R-CNN: A general image manipulation detection model." In 2020 IEEE International Conference on Multimedia and Expo (ICME), pp. 1-6. IEEE, 2020.

[5] Yang, Chao, Zhiyu Wang, Huawei Shen, Huizhou Li, and Bin Jiang. "Multi-Modality Image Manipulation Detection." In 2021 IEEE International Conference on Multimedia and Expo (ICME), pp. 1-6. IEEE, 2021.

[6] Zhou, Peng, Xintong Han, Vlad I. Morariu, and Larry S. Davis. "Learning rich features for image manipulation detection." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1053-1061. 2018.

[7] Wang, Qing, and Rong Zhang. "Double JPEG compression forensics based on a convolutional neural network." EURASIP Journal on Information Security 2016, no. 1 (2016): 1-12.

[8] Gan, Yanfen, and Junliu Zhong. "Research on copy-move image forgery detection using features of discrete polar complex exponential transform." International Journal of Bifurcation and Chaos 25, no. 14 (2015): 1540018.

[9] Li, Ce, Qiang Ma, Limei Xiao, Ming Li, and Aihua Zhang. "Image splicing detection based on Markov features in QDCT domain." Neurocomputing 228 (2017): 29-36.

[10] Verma, Vinay, Nikita Agarwal, and Nitin Khanna. "DCT-domain deep convolutional neural networks for multiple JPEG compression classification." Signal Processing: Image Communication 67 (2018): 22-33.

[11] Nath, S., Naskar, R. Automated image splicing detection using deep CNN-learned features and ANN-based classifier. SIViP 15, 1601–1608 (2021).

[12]Kunj Bihari Meena and Vipin Tyagi 2021 J. Phys.: Conf. Ser. 1714 012038

[12] Zhu, Nan, Junge Shen, and Xiaotong Niu. 2019. "Double JPEG Compression Detection Based on Noise-Free DCT Coefficients Mixture Histogram Model" Symmetry 11, no. 9: 1119. https://doi.org/10.3390/sym11091119

[14] Birajdar GK, Mankar VH. Digital image forgery detection using passive techniques: A survey. Digital investigation. 2013 Oct 1;10(3):226-45.

[15] M. Ali Qureshi and M. Deriche, "A review on copy move image forgery detection techniques," 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14), 2014, pp. 1-5, doi: 10.1109/SSD.2014.6808907.

[16] Qureshi, Muhammad Ali; Deriche, Mohamed (2015). A bibliography of pixel-based blind image forgery detection techniques. Signal Processing: Image Communication, 39(), 46–74. doi:10.1016/j.image.2015.08.008

[17] Hegazi, Aya; Taha, Ahmed; Selim, Mazen M. (2019). An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. Journal of King Saud University - Computer and Information Sciences, (), S1319157819304707–. doi:10.1016/j.jksuci.2019.07.007

[18] Deshpande, Pradyumna, and Prashasti Kanikar. "Pixel based digital image forgery detection techniques." International Journal of Engineering Research and Applications (IJERA) 2, no. 3 (2012): 539-543.

[19] Hayat, Khizar; Qazi, Tanzeela (2017). Forgery detection in digital images via discrete wavelet and discrete cosine transforms. Computers & Electrical Engineering, (), S0045790617305785–. doi:10.1016/j.compeleceng.2017.03.013

[20] Mahmood, Toqeer, Zahid Mehmood, Mohsin Shah, and Tanzila Saba. "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform." Journal of Visual Communication and Image Representation 53 (2018): 202-214.

[21] Gani, Gulnawaz; Qadir, Fasel (2020). A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata. Journal of Information Security and Applications, 54(), 102510–. doi:10.1016/j.jisa.2020.102510

[22] Kaushik, Rajeev, Rakesh Kumar Bajaj, and Jimson Mathew. "On image forgery detection using two-dimensional discrete cosine transform and statistical moments." Procedia Computer Science 70 (2015): 130-136.

[23] Moghaddasi, Zahra, Hamid A. Jalab, and Rafidah Md Noor. "Image splicing forgery detection based on low-dimensional singular value decomposition of discrete cosine transform coefficients." Neural Computing and Applications 31, no. 11 (2019): 7867-7877.

[24] Ojeniyi, Joseph A., Bolaji O. Adedayo, Idris Ismaila, and Shafi'I. Muhammad Abdulhamid. "Hybridized technique for copy-move forgery detection using discrete cosine transform and speeded-up robust feature techniques." (2018).

[25] Kumar, Sunil, Jagannath Desai, and Shaktidev Mukherjee. "A fast DCT based method for copy-move forgery detection." In 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), pp. 649-654. IEEE, 2013.

[26] Alkawaz, Mohammed Hazim, Ghazali Sulong, Tanzila Saba, and Amjad Rehman. "Detection of copy-move image forgery based on discrete cosine transform." Neural Computing and Applications 30, no. 1 (2018): 183-192.

[27] Armas Vega, Esteban Alejandro, Edgar González Fernández, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. "Copy-move forgery detection technique based on discrete cosine transform blocks features." Neural Computing and Applications 33, no. 10 (2021): 4713-4727.

[28] Reddy, V., K. Vaghdevi, and Dr Kolli. "DIGITAL IMAGE FORGERY DETECTION USING SUPER PIXEL SEGMENTATION AND HYBRID FEATURE POINT MAPPING." European Journal of Molecular & Clinical Medicine 8, no. 2 (2021): 1485-1500.

[29] Chen, Haipeng, Xiwen Yang, and Yingda Lyu. "Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm." IEEE Access 8 (2020): 36863-36875.

[30] Li, Weihai, and Nenghai Yu. "Rotation robust detection of copy-move forgery." In 2010 IEEE International Conference on Image Processing, pp. 2113-2116. IEEE, 2010.

[31] Soni, Badal, Pradip K. Das, and Dalton Meitei Thounaojam. "CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection." IET Image Processing 12, no. 2 (2018): 167-178.

[32] Silva, Ewerton, Tiago Carvalho, Anselmo Ferreira, and Anderson Rocha. "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes." Journal of Visual Communication and Image Representation 29 (2015): 16-32.

[33] Hsu, Chih-Chung, Tzu-Yi Hung, Chia-Wen Lin, and Chiou-Ting Hsu. "Video forgery detection using correlation of noise residue." In 2008 IEEE 10th workshop on multimedia signal processing, pp. 170-174. IEEE, 2008.

[34] Bo, Xu, Wang Junwen, Liu Guangjie, and Dai Yuewei. "Image copy-move forgery detection based on SURF." In 2010 International Conference on Multimedia Information Networking and Security, pp. 889-892. IEEE, 2010.

[35] Wu, Yue, Wael Abd-Almageed, and Prem Natarajan. "Busternet: Detecting copy-move image forgery with source/target localization." In Proceedings of the European conference on computer vision (ECCV), pp. 168-184. 2018.

[36] Zheng, Lilei, Ying Zhang, and Vrizlynn LL Thing. "A survey on image tampering and its detection in real-world photos." Journal of Visual Communication and Image Representation 58 (2019): 380-399.

[37] Hashmi, Mohammad Farukh, Vijay Anand, and Avinas G. Keskar. "Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale-invariant feature transform." Aasri Procedia 9 (2014): 84-91.

[38] Wu, Yue, Wael Abd-Almageed, and Prem Natarajan. "Deep matching and validation network: An end-to-end solution to constrained image splicing localization and detection." In Proceedings of the 25th ACM international conference on Multimedia, pp. 1480-1502. 2017.

[39] Zhang, Qingbo, Wei Lu, and Jian Weng. "Joint image splicing detection in dct and contourlet transform domain." Journal of Visual Communication and Image Representation 40 (2016): 449-458.

[40] Rao, Yuan, and Jiangqun Ni. "Self-supervised domain adaptation for forgery localization of JPEG compressed images." In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 15034-15043. 2021.

[41] Vega, Esteban Alejandro Armas, Edgar González Fernández, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. "Passive image forgery detection based on the demosaicing algorithm and JPEG compression." IEEE Access 8 (2020): 11815-11823.

[42] Bo Liu, Chi-Man Pun, Xiao-Chen Yuan, "Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies", The Scientific World Journal, vol. 2014, Article ID 230425, 12 pages, 2014. https://doi.org/10.1155/2014/230425

[43] Hosny, Khalid M., Akram M. Mortda, Mostafa M. Fouda, and Nabil A. Lashin. "An Efficient CNN Model to Detect Copy-Move Image Forgery." IEEE Access 10 (2022): 48622-48632.