An Empirical Study on Copy-Move Forgery Detection Techniques in Images

M. Samel
Research scholar
Department of Computer Science and Engineering
Anurag university,Hyderabad-india-500088
Samuel9859@gmail.com

A. MallikarjunaReddy
Associate Professor,
Department of Computer Science and Engineering
Anurag University-Hyderabad-india-500088
mallikarjunreddycse@cvsr.ac.in

Article Info
Page Number: 183 – 193
Publication Issue:
Vol. 71 No. 3 (2022)

Abstract

Image Forgery is a common practice that can be observed in many of the social networking platforms as memes, animations, fake news, trolls and others. Now days, people in social media platforms got vexed with these fake news because these land them in confusion state. The latest case study in this pandemic is associated with viral news about COVID-19 variants, lockdowns, and vaccinations, which created a lot of tensions among the public. Traditional image processing techniques like PCA, LBP, RBF, and others are popular techniques to identify the forgery images but most of them are unsuccessful while dealing with high dimensionality, noisy, blur images. The people using social network sites need an "Efficient Identification of Copy Move Forgery Detection Techniques" to recognize the fake news. The existing approaches find the overlapped regions to identify the tampered parts in the images but the deep learning mechanisms tries to identify the non-overlapping regions and location parameter optimizations. In this paper, the focus is on various approaches available in the current scenario to detect the forgery parts in the image.

Article History
Article Received: *12 January 2022*
Revised: *25 February 2022*
Accepted: *20 April 2022*
Publication: *09 June 2022*

Keywords: - Tampered Regions, Deep Learning, Copy Move, Wavelet Transformations, HAAR, Dimensionality Reduction

INTRODUCTION:

The image forgery is a process of changing few features in the digital image by performing some manipulations. The classification of image forgery detection mechanisms are presented in figure 1.

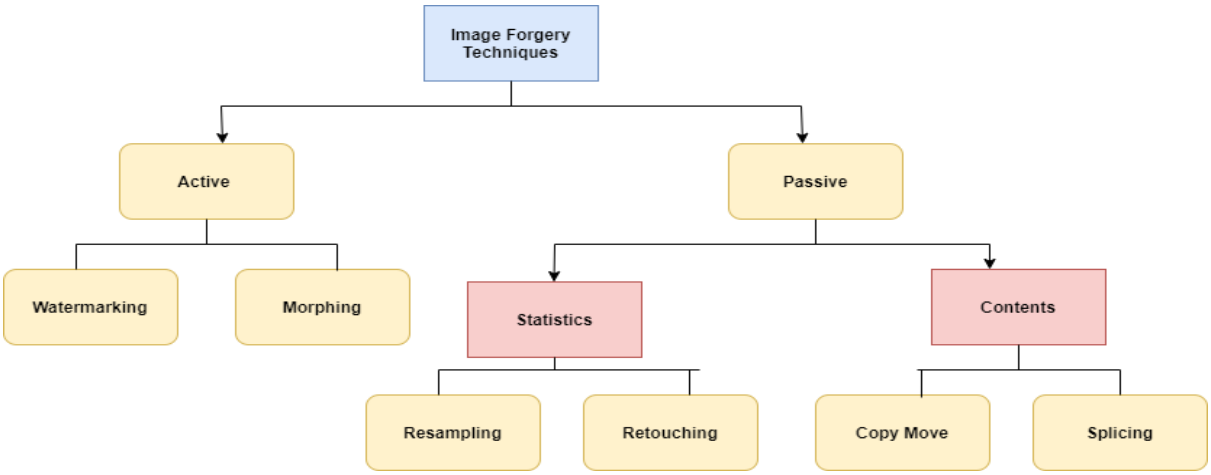

Figure 1: Classification of Image Forgery Techniques

Active techniques are popular in olden days and got a good significance in security applications. Digital signatures, water marking are popular techniques for validating the originality of the image. But these are expensive authentication process because it integrates image with digital signature, during the decoding process, separation of content and image needs more number of resources.

Passive technique is a process of authenticating the image without using any additional resources and the success of this mechanism depends on the assumptions made. Out of four image forgery techniques, geometric techniques got a lot of popularity from the past few decades. In Geometric, the modification of pixels is performed using the "Copy Move", which integrates different parts of different images into one. This copy move process is similar to duplication of images. This process is illustrated using the flow chart as presented in figure 2

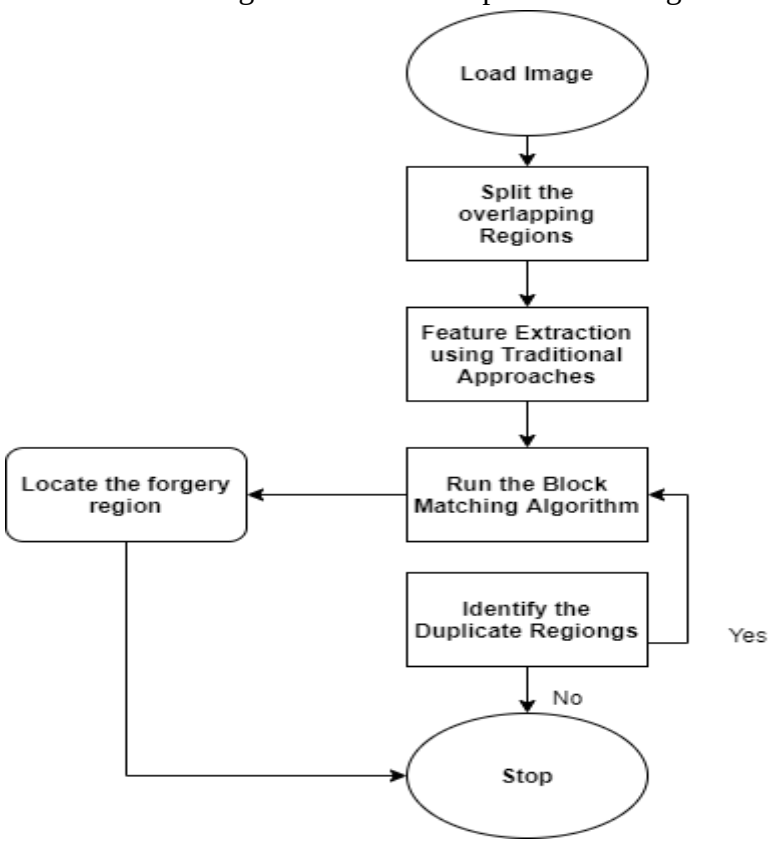

Figure 2: Flow Chart for Copy Move Detection Technique

LITERATURE SURVEY:

In [1] Chi-Man et al proposed adaptive mechanism for over segmentation and matching the features. It is a combination of blocks and key features. In this system, the images are partitioned into blocks of non-overlapping regions and then are labelled based on the matching between the blocks. The model uses an extraction algorithm, in which sub pixels helps to merge the neighbouring blocks based on their similarity to form a region. A merge operation is performed to identify the forgery region. Adaptive mechanism applies SIFT operation on the blocks to extract the points, which are locally matched and considers it as a label. The major advantage of this research lies in the handling of irregular and overlapping blocks. To prevent the loss of information from the overlapped regions and super pixels, it performs clustering adapted with linear functions. To compute the low and high frequencies it performed HAAR integrated DWT for 4 times then a groups of blocks are constructed from the image. This research concentrates on extraction of feature points which can deal even with compressed and restored imagesalso.

In [2] EdoardoArdizzone et aldesigned a matching algorithm based on the triangular key points. This paper extracts the regions in terms of triangles rather than blocks because to extract image along with its contents. Since, geometric transformations are sensitive to shapes; most of the information obtained is accurate and relevant to neighbouring triangles. In this research, images interest points are extracted using an integrated approach of detectors. Using these geometric transformations, like angles are used to explore the colors associated with an image. Vertexes are used to work with the properties of lines. Using the Mean Vector Descriptor (MVD), it computes the inner triangles in the image and from them dominant colors are converted into bins to identify the frequent patterns. The identification of forgery part is performed by designing an adaptive window, which can compare pixels based on threshold.

In [3] DavideCozzolino et al framed an efficient dense field, which focuses on the invariants available as a dense region in the image. This research aims to solve the problems associated with high processing times by integrating the pattern matching technique in the nearest neighbour. In general pattern matching algorithm acts as a linear parameter with randomized property to find dense regions but in this research, pattern matching algorithm is proposed to act as non-linear parameter to search, scale, and rotations. It also solves the problem associated with random offset probability by setting a linear fitting component to N-pixel search technique. This model uses circular harmonic transformations, which considers radial functions and similarity properties into account to extract the features, .During the detection process, this research fine tunes the coefficient wherever necessary to efficiently handle the geometric transformations.

In [4] Wenchang et al, experimented with PSO to improve the copy-move technique to handle the scenarios where, the key point generations are very few from the images. For this, the major reason is more number of important parameters is associated with images. This approach solves this problem by identifying the necessary and crucial parameters dynamically using PSO with the help of SIFT framework based on the image. Initially the model assumes some parameters as necessary and an elemental detection is performed to discard few regions in the image. The image is then converted into RGB and a set of key points descriptors are constructed for finding the matching points based on the affine transformations. This research majorly focuses on estimation of parameters to reduce the complexity by generating a group of key parameters using PSO.

In [5] SHAN JIA et al designed a frame based image copy operation to detect forgery by stabilizing the parameters and finding the optical flow in the images. The main advantage of this research is, it is based on sum consistency to identify the tampered points. From the input video sequence, the model extracts the optical flow then it performs the sum calculation followed by finding the detecting the tampered points, this phase is denoted as "Coarse Detection". In this phase, temporal consistency of the images is checked frame by frame to identify the semantic relation between the scenes in the image. If the video is tempered then by inserting or replacing a frame then this phase can easily detect using this symmetric property. The second phase is called to be "Fine Detection", which involves in identification of duplicate image pairs and then false positive rate is reduced. The purpose fine detection is to find the reason for image forgery i.e., duplicates identification and false detection. This model uses the concept of regularity, which finds the correlation and integrity between two frames.

In [6] Yuanman et al, proposed hierarchical feature matching in which smooth regions are identified by using the contrast threshold method and then images are rescaled. The entire process is designed as a three phase manner in which, the first phase deals with rescaling and contrast threshold, to extract the features. In the second phase to match the points it performs clustering based on the scaling and overlapping. In the third phase, on the regions that are matched it checks for isolation areas by checking the homograph. This model to reduce the key points, it groups the key points as a cluster based on the scaling similarity. The advantage of this technique is, the original matches remain the same. This model also focuses on localization to identify the duplicate regions by validating the homographs and by selecting the dominant angles. In this model, duplicate pairs are isolated by continuously monitoring the regions of the image by adjusting the sliding window.

In [7] Songpon et al, designed a pipelined CMFD process, in which initially the images are pre-processed using LBP integrated with DWT for converting images into gray scale and to remove the noises. This model also deals with dimensionality reduction using the concept of block division segmentation process. In the second stage, the model tries to optimize the key points based on the location of optimization. This model implements a noise added mechanism to identify the duplicate target images then it performs transformations and rotations. Using transformations, the images are converted into frequencies and a feature descriptor is generated, then it is passed to next stage of feature extraction to map the features based on pattern matching and the process is re-iterated until the error rate is refined to minimum level. The model adapts ORSA mechanism to remove the false positives where the non-tampered regions are considered as the defected parts. Finally, it performs localization to improve the quality of the image.

In [8] Haipeng et al, integrated neighbouring search with keypoints to identify the similarity between the images. The keypoints of the images are clustered based on different parameters to reduce the time complexity from O(n*n) and a hierarchical representation of color, then scale and then overlapping areas are performed. The major goal of the clustering is to maximize the differences between the keypoints by forming an octave pair. Based on RGB color, this octave forms 24 pairs (8*3). These features are presented using SIFT because it is popular for representing the images in different scaling factors and the features extracted will not be affected by any sort of transformations. The mismatches in the images are removed by J-Linkage algorithm. To identify the tampered regions, this model implements neighbor search to localize the regions. It performs affine transformations integrated with PCA to mark the seed in the corresponding points.

In [9] Mahmood et al, studied about forensic analysis DCT integrated with Gaussian kernels. It performs a lot of post processing operations to identify the forgery regions that involved in blur, compression, and noise. The model initially converts into gray scale. DCT's are applied to perform rotations on each block to produce nominal data. DCT constructs a coefficient matrix to identify whether it is a tampered block or not. All the tampered blocks are ignored for future processing and this reduces the number of blocks for final accessing. PCA is integrated with kernel to obtain the non-linear relations between the blocks because it is good in designing the hyper parameters for the model [16-19]. The model then identifies the semantic similarity between the blocks by constructing the Gamma matrix with the help of Eigen values then the matrix is sorted to identify the closeness between the blocks.

In [10] VEGA et al, implemented demosaicing passive techniques to detect forgery in compressed images. Error level technique analysis the different compression applied on the image. ELA concludes that higher the error level higher will be the manipulation operations on the image. It applies color filter to find the interpolation patterns then it converts the RGB color intensities into binary based on the location. It computes the error rate MSE are computed by re-interpolating the color pixels. The filter operation is performed using the median because median are resistant to both high and low resolutions. For the images received through sensors, instead of median filter, this model applies chromatic interpolation. Any noise obtained in the sensor data is removed through wavelet transformations. These filtered images are then passed as input to the demosaicing algorithm to perform the splice operation.

In [11] Biach et al, designed encoder based CNN known as "Fals-Unet" to identify the manipulations performed on the images which are not visually available. Using ResNet-50, it explores spatial maps characteristics and uses decoder to reconstruct the low resolution images by concatenating two dense layers as one. A block is constructed for encoder to enhance the high level features by including CNN, Activation, and normalization. Since this models works with spatial images, the size of the kernel and filter varies from layer to layer. The encoder block contains 4 residual components which not only improves the optimization parameters but also solves the problem of complexity even though the number of layers increases in the model. The decoder solves the unbalanced class by assigning the weights to the blocks based on spliced regions and pool pixels. Finally, the similarities are computed using Matthews and Jaccard Coefficients.

In [12] Chen et al, proposedsemantic matching through reinforcement technique application on hybrid features. All the features are re-sampled using LSTM to identify the patches and amplifying the tampered and un-tampered regions. The images are transformed using the radonoperations and it is passed through the stacked layers to extract the semantic features. These features are rotated for 4 times using residual components andhybrid features are concatenated with fusion features to predict the mask. The LSTM composed of three gates to control the flow of inputs through different activation functions attached to them. In this model, decoding block also contains residual components associated with heat maps and model is fine tuned to find the results for the ground truth images[21-23].

In [13] Neeraj Kumar et al, designed SVD combined with Bi-orthogonal WT for image forgery detection. SVD extracts the image block by block and duplicate regions are identified. The model constructs clone vectors by computing the similarities through minkoswki distance. Wavelet and filter transformations are applied to obtain semantic similarities between blocks. To identify the damaged images or manipulated parts it applies spline wavelets and images are reconstructed. IRVM

authenticates the image by checking the glow warm parameters at each step and updates the weights accordingly. The objective of the glow warm function is to minimize the error rate by moving in unique direction and taking the decisions based on the local regions. The block matching is performed to identify the forgery areas.

In [14] Anuja et al, affine transformations are attached to the reflection techniques to identify the most frequently tampered regions. Center Surround is applied to extract the keypoints in the image like corners, edges, colors and shapes and Extrema is applied to find the local regions though searching process. Different filters like star are applied to find the changes in the rotated image, bi-level is applied to identify the duplicate values, and non-maximal is applied to identify the magnitude differences. Feature descriptors are computed using Euclidian distance to check the threshold level.

In [15] N. Krishnaraj et al, implemented fusion model using deep learning with a first motive to generate more number of forgery images using advanced GAN's and second motive is to construct a DenseNet to classify the image as tampered or not [24]. The DenseNet requires very less parameters to estimate so the model applies transfer learning to reutilize all the features necessary to identify the manipulations. ELM is attached as activation function to the binary classifier layer to take decision based on the large area covered by the network [25].

Table 1: Analysis on the Existing Scenarios

S.No	Author	Algorithm	Merits	Demerits/ Limitations
1	Chi-Man	Forgery Region Extraction (FRE)	The model can handle the non polygon shaped regions and overlapping blocks efficiently	Initialization of super pixel values is an expensive and complicated process.
2	EdoardoArdizzone	Triangulation of Key Points	It predicts the tampered regions by integrating normalization process in the MVD, which makes detection process easy.	The number of regions based on the triangular shape is less and provides more amount of irrelevant data.
3	DavideCozzolino	Efficient Dense Field	Matching algorithms can efficiently handle the invariants features. It solves the real time problems by constructing a four dimensional space	Algorithm needs more iterations to handle four dimensional space and it is inefficient in handling the patch interpolation in images
4	Wenchang	CMFD-PSO	Using PSO techniques, this research tries to reduce the number of parameters during the training phase	This model cannot handle images with low resolution and its accuracy rate is very low when the image contains uniform texture
5	Shan Jia	Coarse to fine	Optical flow points help the model to suspect the tempered points easily.	This model cannot handle dynamic scenario scenes efficiently

			It can also handle the duplicate images by finding the OF correlation	
6	Yuanman	Hierarchical Feature Matching	The localization parameters attached to this model explores the necessary properties	This model suffers from dense field optimization problem while handling the color images
7	Songpon	CMFD pipeline architecture	The model identified the drawbacks in general approach then it applied pipeline mechanism for those stages.	Checking all the mechanisms associated with each stage and picking the appropriate one is a time consuming process.
8	Haipeng	Neighbouring keypoints	In this model, localization algorithm focuses more on the tampered data, which manipulated using complex operations	The model uses affine transformations for expanding the head elements of the queue, which contains keypoints. So, a better data structure is needed
9	Mahmood	DCT+Kernels	Gram matrix helps to find the semantic relation and judge the neighbouring blocks for closeness	The model can be extending by constructing tensor vectors instead of traditional matrices to find the similarity
10	VEGA	Demosaicing Algorithm	The error rate in the compressed images reduced a lot.	The results obtained through splice operation needs an n*n matrix to represent.
11	Biach	Fals-Unet	The manipulation of images are recognized through manipulation identification by mapping spatial masks	It attempts to identify only the false regions in the image
12	Chen	Semantic Reinforcement	Heat maps helps the model to configure the layers dynamically	The mechanism for selecting the hybrid features through traditional approaches made it inefficient
13	Neeraj Kumar	BWT-SVD	In traditional approaches, denoising is performed through	Whenever the local region is modified the domain in the global warm should be

			complex operations but here, it applies simple statistics to achieve the necessary task	updated and the entire process should be initiated from zero

Research Gaps Identified:

1. The model needs to identify the automation algorithm which can deal with both linear and non-linear shapes.
2. The model needs to address the images with more intensity, different colors, more number of manipulations, and others with optimistic design and less cost.
3. The model should be able to distinguish between super pixels and manipulated pixels using deep learning approaches.

Observations:

The paper studied about number of existing algorithms and chalked out all the performance measures of different algorithms and presented in table 2 to identify the efficient approach and to extend it further in future work.

Table 2: Accuracy Analysis of Baseline Works

S.No	Algorithm	Accuracy	Precision	Recall
1	Forgery Region Extraction (FRE)	97.72	97.22	83.73
2	Triangulation of Key Points (TKP)	91.8	89	86.31
3	Efficient Dense Field (EDF)	93.4	90.7	90.7
4	CMFD-PSO	98.9	100	100
5	Coarse to fine	83.7	80.6	81.98
6	Hierarchical Feature Matching	99.10	98.9	100
7	CMFD pipeline architecture	96.9	97.1	94.3

Figure 3 presents the accuracy, recall, and precision of the existing algorithm, which are crucial parameters for the machine learning algorithms. In the figure X-axis denotes the algorithms and Y-axis represents the percentage measurement of all the three metrics.

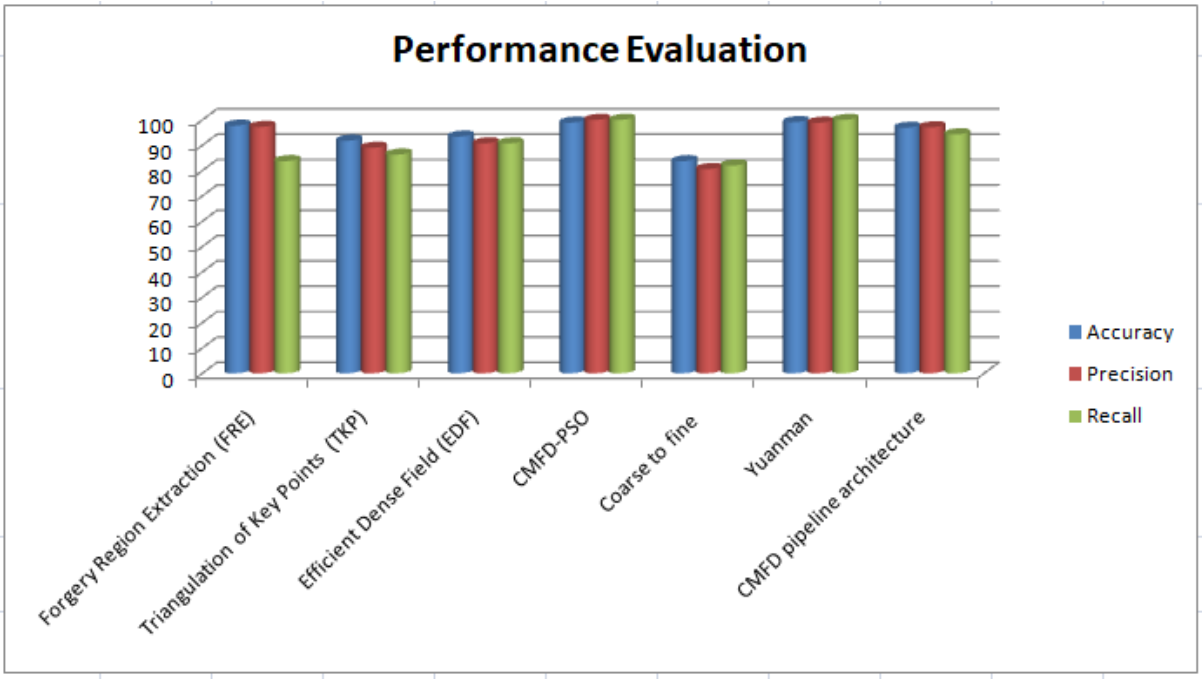

Figure 3: Analysis on Performance Metrics

Conclusion:

The protection of images in the digital media platform has become a challenging task now days due to the availability of image morphing applications available in the market. The proposed paper studies about the various image forgery techniques that are available under copy move technique and identified that "Hierarchical Feature Matching" algorithm has a significance impact on the authentication provision. Based on this mechanism, in future work, the model can be extended by integrating it with the deep learning algorithms which pre-trained models, fine tuning of the layers, and transfer learning to further improve the advantages of the model.

REFERENCES:

1. C. -M. Pun, X. -C. Yuan and X. -L. Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1705-1716, Aug. 2015, doi: 10.1109/TIFS.2015.2423261.
2. E. Ardizzone, A. Bruno and G. Mazzola, "Copy–Move Forgery Detection by Matching Triangles of Keypoints," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2084-2094, Oct. 2015, doi: 10.1109/TIFS.2015.2445742.
3. D. Cozzolino, G. Poggi and L. Verdoliva, "Efficient Dense-Field Copy–Move Forgery Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284-2297, Nov. 2015, doi: 10.1109/TIFS.2015.2455334.
4. S. Wenchang, Z. Fei, Q. Bo and L. Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques," in *China Communications*, vol. 13, no. 1, pp. 139-149, Jan. 2016, doi: 10.1109/CC.2016.7405711.
5. S. Jia, Z. Xu, H. Wang, C. Feng and T. Wang, "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics," in *IEEE Access*, vol. 6, pp. 25323-25335, 2018, doi: 10.1109/ACCESS.2018.2819624.

6. Y. Li and J. Zhou, "Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1307-1322, May 2019, doi: 10.1109/TIFS.2018.2876837.
7. S. Teerakanok and T. Uehara, "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," in *IEEE Access*, vol. 7, pp. 40550-40568, 2019, doi: 10.1109/ACCESS.2019.2907316.
8. H. Chen, X. Yang and Y. Lyu, "Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm," in *IEEE Access*, vol. 8, pp. 36863-36875, 2020, doi: 10.1109/ACCESS.2020.2974804.
9. ToqeerMahmood, Tabassam Nawaz, AunIrtaza, Rehan Ashraf, Mohsin Shah, Muhammad Tariq Mahmood, "Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images", *Mathematical Problems in Engineering*, vol. 2016, Article ID 8713202, 13 pages, 2016. https://doi.org/10.1155/2016/8713202
10. E. A. Armas Vega, E. González Fernández, A. L. Sandoval Orozco and L. J. GarcíaVillalba, "Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression," in *IEEE Access*, vol. 8, pp. 11815-11823, 2020, doi: 10.1109/ACCESS.2020.2964516.
11. El Biach, F.Z., Iala, I., Laanaya, H. et al. Encoder-decoder based convolutional neural networks for image forgery detection. Multimed Tools Appl (2021). https://doi.org/10.1007/s11042-020-10158-3
12. Chen, H., Chang, C., Shi, Z., &Lyu, Y. (2021). Hybrid features and semantic reinforcement network for image forgery detection. Multimedia Systems. doi:10.1007/s00530-021-00801-w
13. Rathore, N. K., Jain, N. K., Shukla, P. K., Rawat, U., &Dubey, R. (2020). Image Forgery Detection Using Singular Value Decomposition with Some Attacks. National Academy Science Letters. doi:10.1007/s40009-020-00998-w
14. Dixit, A., & Bag, S. (2021). A fast technique to detect copy-move image forgery with reflection and non-affine transformation attacks. Expert Systems with Applications, 182, 115282. doi:10.1016/j.eswa.2021.115282
15. N. Krishnaraj, B. Sivakumar, RamyaKuppusamy, YuvarajaTeekaraman, Amruth Ramesh Thelkar, "Design of Automated Deep Learning-Based Fusion Model for Copy-Move Image Forgery Detection", Computational Intelligence and Neuroscience, vol. 2022, Article ID 8501738, 13 pages, 2022. https://doi.org/10.1155/2022/8501738.
16. Sudheer Reddy, K., Varma, G.P.S., Reddy, S.S.S., Understanding the scope of web usage mining & applications of web data usage patterns, 2012 International Conference on Computing, Communication and Applications, ICCCA 2012.
17. A Mallikarjuna Reddy, VakulabharanamVenkata Krishna, LingamguntaSumalatha and AvukuObulesh, "Age Classification Using Motif and Statistical Features Derived On Gradient Facial Images", Recent Advances in Computer Science and Communications (2020) 13: 965. https://doi.org/10.2174/2213275912666190417151247.
18. Mallikarjuna Reddy, A., RupaKinnera, G., Chandrasekhara Reddy, T., Vishnu Murthy, G., et al., (2019), "Generating cancelable fingerprint template using triangular structures", Journal of Computational and Theoretical Nanoscience, Volume 16, Numbers 5-6, pp. 1951-1955(5), doi: https://doi.org/10.1166/jctn.2019.7830.
19. Swarajya Lakshmi V Papineni, SnigdhaYarlagadda, HaritaAkkineni, A. Mallikarjuna Reddy. Big Data Analytics Applying the Fusion Approach of Multicriteria Decision Making with Deep Learning

Algorithms *International Journal of Engineering Trends and Technology*, 69(1), 24-28, doi: 10.14445/22315381/IJETT-V69I1P204.

20. A.Mallikarjuna, B. KarunaSree, " Security towards Flooding Attacks in Inter Domain Routing Object using Ad hoc Network" International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-3, February 2019.
21. Mallikarjuna Reddy, A.,Venkata Krishna, V. and Sumalatha, L." Face recognition approaches: A survey" International Journal of Engineering and Technology (UAE), 4.6 Special Issue 6, volume number 7 , 117-121,2018.
22. C. R. T, G. Sirisha and A. M. Reddy, "Smart Healthcare Analysis and Therapy for Voice Disorder using Cloud and Edge Computing," *2018 4th International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Mangalore, India, 2018, pp. 103-106, doi: 10.1109/iCATccT44854.2018.9001280.
23. IlaiahKavati, A. Mallikarjuna Reddy, E. Suresh Babu, K. Sudheer Reddy, RamalingaSwamyCheruku,Design of a fingerprint template protection scheme using elliptical structures,ICTExpress,Volume 7, Issue 4,2021,Pages 497-500,ISSN 2405-9595,https://doi.org/10.1016/j.icte.2021.04.001.
24. Ayaluri MR, K. SR, Konda SR, Chidirala SR. 2021. Efficient steganalysis using convolutional auto encoder network to ensure original image quality. PeerJ Computer Science 7:e356 https://doi.org/10.7717/peerj-cs.356.
25. Swarajyalakshmi v papineni, A.Mallikarjuna Reddy, Sudeeptiyarlagadda , SnigdhaYarlagadda, HarithaAkkineni *"An Extensive Analytical Approach on Human Resources using Random Forest Algorithm"* International Journal of Engineering Trends and Technology 69.5(2021):119-127.