Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 5): pp. 1802-1809
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.198

A Supervised learning neural network based approach for image splicing

Kavita Rathi*, Faculty, CSED, Deenbandhu Chhotu Ram University of Science & Technology, Sonipat, Haryana, India
Parvinder Singh, Faculty, CSED, Deenbandhu Chhotu Ram University of Science & Technology, Sonipat, Haryana, India

ABSTRACT- An efficient supervised learning approach for splicing forgery detection with low classification error rates is proposed in this work. Existing Literature is analysed to produce the research gap and and PCA is used for feature extraction to make the detection process fast and intelligent. As PCA is the process of dimension reduction without eliminating the significant information from the image. Canny edge detection is used to detect strong edges in the image. . Back propagation neural networks Model for classification is trained by feeding dataset images. A benchmark dataset CASIA V2 is used for evaluating performance of proposed algorithm. The images are then tested for authenticity, whether the image is forged or authentic. Then the performance is evaluated by using parameters like precision, Recall and Mean Square Error. Proposed approach is able to increase the accuracy with low classification error rate while the existing work takes the optimal value to get their required result. Simulation results for the proposed algorithm are presented.

Keywords: Neural network, image forgery detection, dataset, edge detection, feature extraction, authenticity

I. INTRODUCTION

Image Forgery is a type of cybercrime on digital images (real image is modified). Manipulator also wants manipulations to be undetectable. There are two basic approaches to detect forgery Active and Passive Forgery Detection Techniques. Paper will focus on Passive Techniques. ACTIVE APPROACH: In active approach, digital signature and watermarking is used to identifying the originality of an image. PASSIVE APPROACH: Passive approach is also known as blind approach. In this forensic there is no need of prior information about an image. Passive approach is based upon different processing methods with the help of these methods forged, manipulation piece of an image are detected.

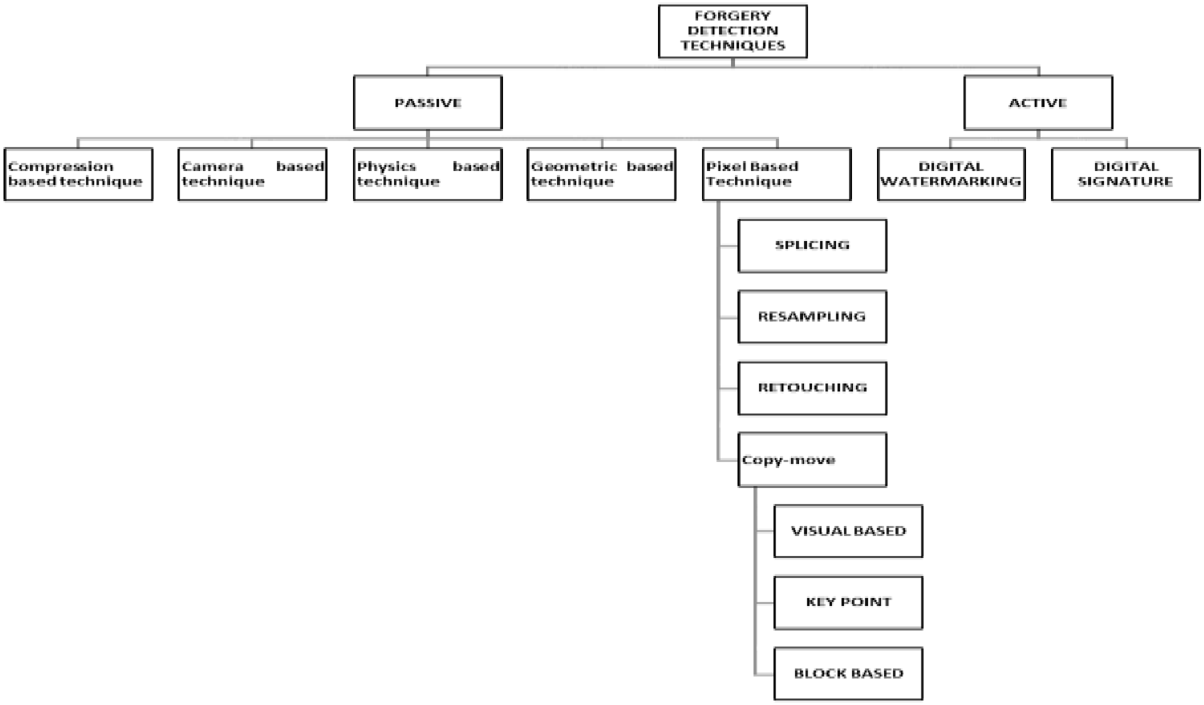


Fig. 1: Forgery Detection Techniques

II. Literature Review

Different Key Point Based Algorithms: SIFT (Scale invariant Feature Transform) A robust and distinctive descriptor. It is an algorithm to detect local features in an image. It is efficient in object recognition but it failed in real time applications.[3] SURF [4] Wavelet Transform and SURF [5][6] KAZE are two dimensional feature detectors. It helps in reducing noise and at the same time helps in maintaining boundaries. It uses nonlinear scale space. Harris corner points: It is used for finding corner points by matching the difference in intensities for displacement in all directions. [7] BRISK (Binary Robust Invariant Scalable Key points). It relies on circular sampling pattern to compute brightness comparisons. Plane, rotation attacks makes it unsuitable. [8] MIFT (Modified Iterative Fourier Transform) [9][10] JLinkage It is used in matching and generating multiple local homography hypotheses.[11] SIFER (Scale Invariant Feature Detector with Error Resilience) It uses Cosine Modulated Gaussian filter [12] FAST (Features from accelerated segment test) It tells us about the presence of a corner by testing a circular area.

Block Based Algorithms: DCT (Discrete Cosine Transform): It is used for converting the image into frequency domain. [13] DWT (Discrete Wavelet Transform) : It allows time and frequency analysis of images. It is used for images having discontinuous edges. [14] DSWT (Discrete stationary Wavelet transform) it is used in combination with DCT to separate the colors.[15] PCA It is sensitive to noise. It is an efficient method and gives low false positives.[16] FMT: An efficient algorithm which can work with noise, compressions, scaling but is unable to work properly if image is highly rotated. [17] Zernike Moments: They represent images without repetition or commonality of information between the moments. It is also used for feature extraction.[18] CCV (Color Coherence Vector) it is used for fast multiresolution image querying with increased speed of the image retrieval. [19] LBP (Local Binary Pattern) It describes each pixel by relative grey scale levels of its neighbor's pixels. It has faster computational power and is invariant to monotonic illumination variations. [20] SVD (Singular Value Decomposition) [21] DCT [22] FMT (Fourier Melin Transform) [23] Kernel Principal Component Analysis [24] Blur Moment Invariant: It is robust against blur/noise and compressions. [25] MDS (Multidimensional Scaling) It extracts a rotation invariant DFT feature matrix with log polar transform and is impervious to angle rotations. [26] LFD (Local Fractal Dimension) [27] DFT (Direction Filter Technique). It works for both compressed and uncompressed images.

No focus has been made on all types of attacks in present techniques and to solve the problems optimization are made for high precision and classification error rates which gave deep motivation to proposed work. The existing work is done on the segmentation of the processed images but very less light on reducing the loss functions for high performance evaluation in the detection of the forgeries. Therefore, the proposed approach try to overcome this problem by achieving high accuracy rate and low misclassifications.

III. Proposed System

Proposed Approach is divided into following modules:

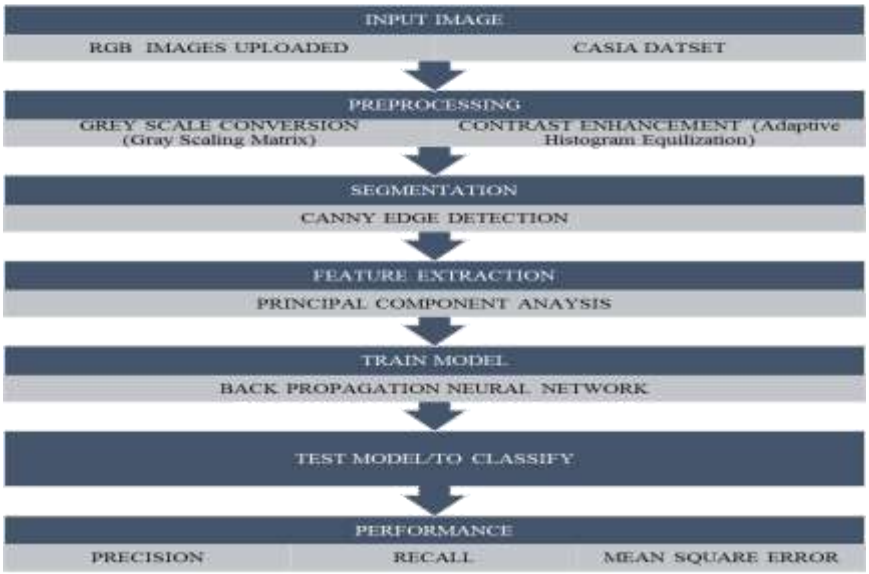


Fig. 2: Workflow diagram

3.1 Input Image

The RGB iamge is uploaded using MATLAB function. Once the image is uploaded it is converted into a 3x3 matrix.

3.2 Preprocessing

There are different kinds of techniques for image processing such that gray scale transformation, geometric transformation, image resizing, image restoration, image enhancement etc. This paper uses Grayscale conversion and Contrast Enhancement.[28] Grayscale Conversion is done using Uploading Grey level Conversion scheme. In this the image is converted from RGB to Grayscale to reduce the amount of space used and to reduce the complexity which is associated with three channel system.

3.3 Segmentation

Edge Detection does contrast level Enhancement. Different enhancement techniques are there like removal of noise, different types of filterslike average filter,gaussian filter,etc. Various functions used for contrast enhancement are imadjust,histeq and adapthisteq [29][30]. In this work adapthisteq function is used.

3.4 Feature Extraction

Feature Extraction is the property of dimension reduction without eliminating the significant information from the data. So, for this purpose PCA (Principal Component Analysis) is used [31][32].

3.5 Training Neural Network Model

Backpropagation neural network is used to train the data. A benchmark dataset is always required for evaluating performance of algorithms therefore CASIA V2 dataset is fed to the network for training purpose[33][34]. This dataset is freely available on the internet. In this dataset images are in true colour or RGB Scale and are forged with Splicing.

3.6 Testing Images

The images are then tested for authenticity, means whether the tested image is forged or authentic with the help of Classification (matching) [35][36].

3.7 Performance Evaluation

Performance evaluation is done by using parameters like precision, Recall, accuracy and Mean Square Error.

3.8 Algorithm

Step 1: Get Training samples I_x such that

{$I_{x=}$ I_1, I_2 I_3 - - I_n}

Step 2: Convert I_x to G_x such that ,G_x = rgb2gray (I_x) &G_x = {G_1, G_2, G_3 - - - G_n}

Step 3: perform Contrast level Enhancement $C_{x,\text{ such}}$ that C_x = F (contrast (G_x)) where, Cx = Enhanced Intensity Image.i.e Cx = {C_1,C_2, C_3... C_n}.

Step 4: Get the edge boundaries using Edge detection E_x such that

E_x = Edge (C_{x1}, C_{x2}, $C_{x3\dots}$ C_{xn})

Step 5: Perform the feature Extraction & Extract feature vector such that.

F_x=for i=1 to n. Extract {f(x)}

END for

Step 6: Save f(x) in the matrix M(x)

Step 7: Train the model for all the I_m, where I_m = Image includes all Training set

Step 8: Generate Test Sample (T_x) such that T_x={T_1, T_2, 7_3… T_n}

Step 9: Load T_m such that T_m = Trained Model

Step 10: Perform classification or Matching such that C_D= classify (T_M, T_f)

Where, T_M = Trained Model feature

T_f = Test Extracted feature for classification

Step 11: Perform Evaluation and stop

IV. Stimulation Result and Analysis

The experiment is implementd using MATLAB 2017b on computer with i3 processor and 8 GB of RAM.

4.1 Dataset

CASIA: It is widely used dataset for evaluating multiple types of attacks. CASIA dataset consists of uncompressed images and JPEG images with different compression quality factor. It consist of 7491 forged images and 5123 original images [1][2][3][5][7][8].Splicing images and post processing images are also used.

4.2 Evaluation Metrics: Performance evaluation

Precision, recall and F1- measure are used as evaluation metrices [21]:

Precision= TP/TP+FP

Recall= TP/TP+FN

F1-measure=2x (precision x recall) / precision + recall

4.3 Results

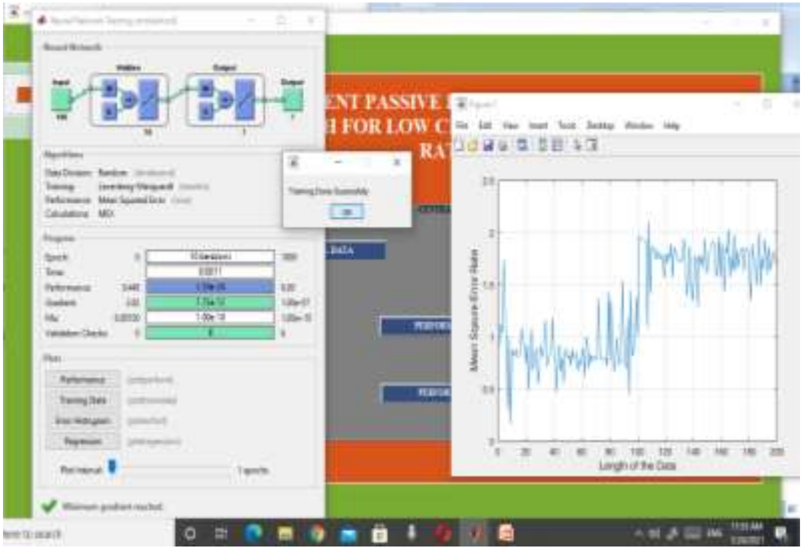


Fig. 3: Neural Network Training

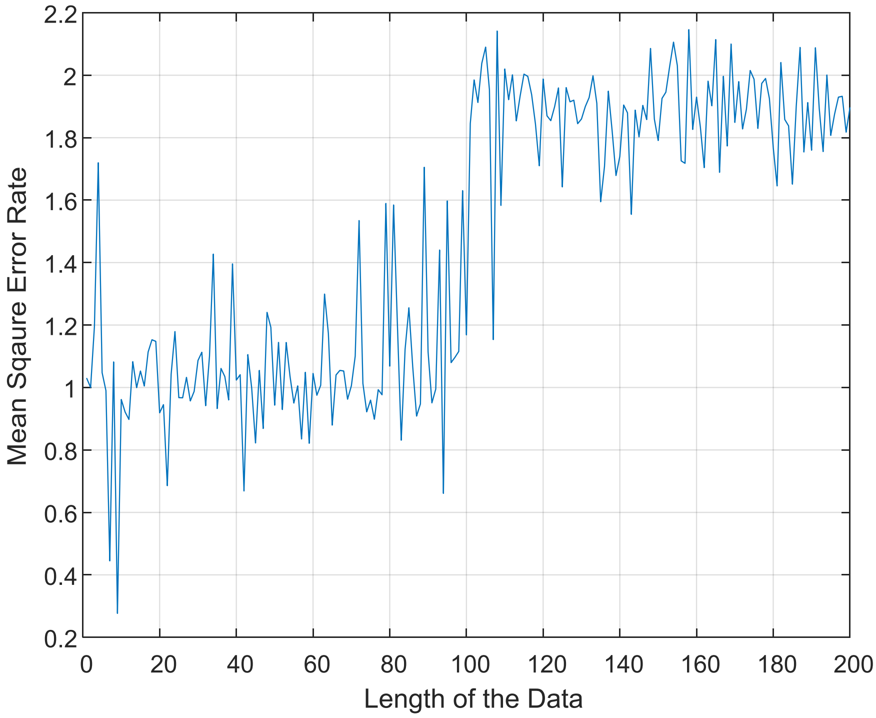
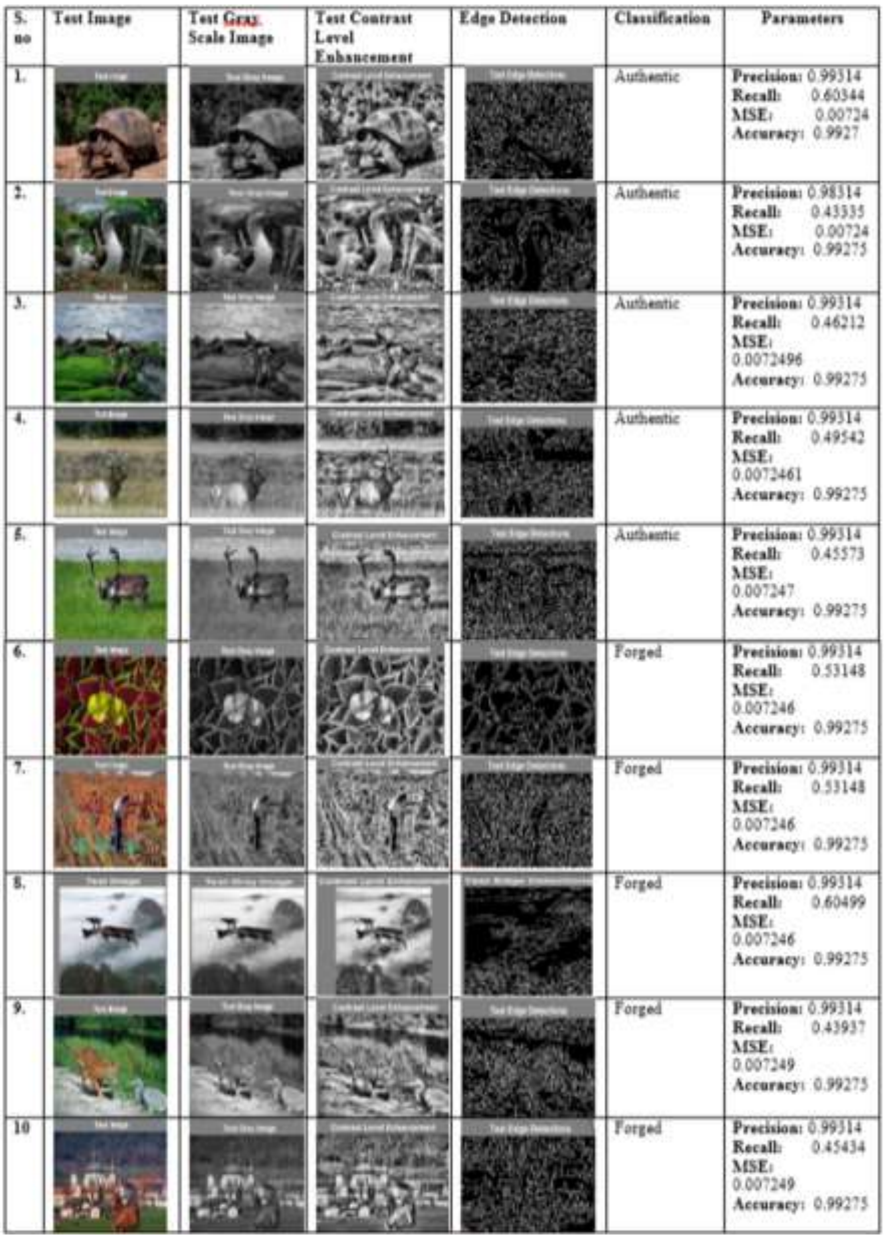


Fig. 4: MSE vs. Length of data



S. no	Test Image	Test Gray Scale Image	Test Contrast Level Enhancement	Edge Detection	Classification	Parameters
1.					Authentic	**Precision:** 0.99314 **Recall:** 0.60344 **MSE:** 0.00724 **Accuracy:** 0.9927
2.					Authentic	**Precision:** 0.98314 **Recall:** 0.43335 **MSE:** 0.00724 **Accuracy:** 0.99275
3.					Authentic	**Precision:** 0.99314 **Recall:** 0.46212 **MSE:** 0.0072496 **Accuracy:** 0.99275
4.					Authentic	**Precision:** 0.99314 **Recall:** 0.49542 **MSE:** 0.0072461 **Accuracy:** 0.99275
5.					Authentic	**Precision:** 0.99314 **Recall:** 0.45573 **MSE:** 0.007247 **Accuracy:** 0.99275
6.					Forged	**Precision:** 0.99314 **Recall:** 0.53148 **MSE:** 0.007246 **Accuracy:** 0.99275
7.					Forged	**Precision:** 0.99314 **Recall:** 0.53148 **MSE:** 0.007246 **Accuracy:** 0.99275
8.					Forged	**Precision:** 0.99314 **Recall:** 0.60499 **MSE:** 0.007246 **Accuracy:** 0.99275
9.					Forged	**Precision:** 0.99314 **Recall:** 0.43937 **MSE:** 0.007249 **Accuracy:** 0.99275
10					Forged	**Precision:** 0.99314 **Recall:** 0.45434 **MSE:** 0.007249 **Accuracy:** 0.99275

Fig. 5: Simulation Results

V. Conclusion

There are different kind of techniques available for image manipulation; Splicing is one of them. An efficient supervised learning approach for splicing forgery detection with low classification error rates is proposed in this work. Then the performance is evaluated by using parameters like precision, Recall and Mean Square Error. Proposed approach is able to increase the accuracy with low classification error rate while the existing work takes the optimal value to get their required result. Less false positive and false negative rate and more precision, recall rate shows that the Proposed approach is able to increase the accuracy while the existing work takes the optimal value to get their required result. More parameters are used to make comparisons more realistic.

References

1. Al-Qershi, Osamah M., and Bee Ee Khoo. "Evaluation of copy-move forgery detection: datasets and evaluation metrics." Multimedia Tools and Applications 77.24 (2018): 31807-31833.
2. Zhang, Zhi, Chengyou Wang, and Xiao Zhou. "A survey on passive image copy-move forgery detection." Journal of Information Processing Systems 14.1 (2018): 6-31.

3. Xiao, Bin, et al. "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering." Information Sciences 511 (2020): 172-191.
4. Yıldırım, Esra Odabaş, and Güzin Ulutaş. "Augmented features to detect image splicing on SWT domain." Expert Systems with Applications 131 (2019): 81-93.
5. Parveen, Azra, Zishan Husain Khan, and Syed Naseem Ahmad. "Block-based copy–move image forgery detection using DCT." Iran Journal of Computer Science 2.2 (2019): 89-99.
6. Shah, Atif, and El-Sayed M. El-Alfy. "Multi-scale LPQ-DCT for Image Forgery Detection." 2019 8th International Conference on Modeling Simulation and Applied Optimization (ICMSAO). IEEE, 2019.
7. Asghar, Khurshid, et al. "Edge–texture feature-based image forgery detection with cross-dataset evaluation." Machine Vision and Applications 30.7 (2019): 1243-1262.
8. E. Isha and E. V. Goyal, "A literature review of Image Forgery Detection," Int. J. Res. Appl. Sci. Eng. Technol., vol. 4, no.IX, pp. 75–80, 2016.
9. [9] Kashyap, Abhishek, et al. "An evaluation of digital image forgery detection approaches." arXiv preprint arXiv:1703.09968 (2017).
10. Parveen, Azra, Zishan Husain Khan, and Syed Naseem Ahmad. "Block-based copy–move image forgery detection using DCT." Iran Journal of Computer Science 2.2 (2019): 89-99.
11. Bae, Seong-jun, and Song Chong. "TCP-friendly flow control of wireless multimedia using ECN marking." Signal Processing: Image Communication 19.5 (2004): 405-419.
12. Christlein, Vincent, Christian Riess, and Elli Angelopoulou. "A study on features for the detection of copy-move forgeries." Sicherheit 2010. Sicherheit, Schutz und Zuverlässigkeit(2010).
13. Cox, Ingemar J., et al. Digital watermarking. Vol. 53. San Francisco: Morgan Kaufmann, 2002.
14. Kumar, B. Santhosh, et al. "A systematic study of image forgery detection." Journal of computational and theoretical Nanoscience 15.8 (2018): 2560-2564.
15. Walia, Savita, and Krishan Kumar. "Digital image forgery detection: a systematic scrutiny." Australian Journal of Forensic Sciences 51.5 (2019): 488-526.
16. Sadeghi, Somayeh, et al. "State of the art in passive digital image forgery detection: copy-move image forgery." Pattern Analysis and Applications 21.2 (2018): 291-306.
17. Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. "Copy-move forgery detection via texture description." Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence. 2010.
18. Sahay, Ajay, and Anupama Gautam. "Comparison between SIFT and SURF image forgery Algorithms." International Journal of Computer Applications 164.2 (2017): 9-11.
19. Hashmi, Mohammad Farukh, and Avinash G. Keskar. "Fast and robust copy-move forgery detection using wavelet transforms and SURF." Int. Arab J. Inf. Technol. 16.2 (2019): 304-311.
20. Abdel-Basset, Mohamed, et al. "2-Levels of clustering strategy to detect and locate copy-move forgery in digital images." Multimedia Tools and Applications 79.7 (2020): 5419-5437.
21. Puri, Malti, and Vinay Chopra. "A Review: Block-Based Copy-Move Forgery Detection Methods."
22. Lamba, Amanjot Kaur, Neeru Jindal, and Sanjay Sharma. "Digital image copy-move forgery detection based on discrete fractional wavelet transform." Turkish Journal of Electrical Engineering and Computer Science 26.3 (2018): 1261-1277.
23. Fan, Ruiqin, et al. "Smart Image Enhancement Using CLAHE Based on an F-Shift Transformation during Decompression." Electronics 9.9 (2020): 1374.
24. Kalbasi, Mahdi, and Hooman Nikmehr. "Noise-Robust, Reconfigurable Canny Edge Detection and its Hardware Realization." IEEE Access 8 (2020): 39934-39945
25. Chatterjee, Sayan, et al. "Retinal Blood Vessel Segmentation Using Edge Detection Method." Journal of Physics: Conference Series. Vol. 1717. No. 1. IOP Publishing, 2021
26. Malbog, Mon Arjay F., et al. "Edge Detection Comparison of Hybrid Feature Extraction for Combustible Fire Segmentation: A Canny vs Sobel Performance Analysis." 2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC). IEEE, 2020.
27. Park, Keumsun, Minah Chae, and Jae Hyuk Cho. "Image Pre-Processing Method of Machine Learning for Edge Detection with Image Signal Processor Enhancement." Micromachines12.1 (2021): 73
28. Shah, Ali Akbar, et al. "Real time identification of railway track surface faults using canny edge detector and 2D discrete wavelet transform." Annals of Emerging Technologies in Computing (AETiC) 4.2 (2020): 53-60.
29. Tripathy, Sushreeta, and Tripti Swarnkar. "Unified preprocessing and enhancement technique for mammogram images." Procedia Computer Science 167 (2020): 285-292.
30. Chandrashekar, Leena, and A. Sreedevi. "A Multi-Objective Enhancement Technique for Poor Contrast Magnetic Resonance Images of Brain Glioblastomas." Procedia Computer Science 171 (2020): 1770-1779.
31. Dar, Khursheed Ahmad, and Sumit Mittal. "An Enhanced Adaptive Histogram Equalization Based Local Contrast Preserving Technique for HDR Images." IOP Conference Series: Materials Science

and Engineering. Vol. 1022. No. 1. IOP Publishing, 2021.

32. Ningsih, Dwi Ratna. "Improving Retinal Image Quality Using the Contrast Stretching, Histogram Equalization, and CLAHE Methods with Median Filters." International Journal of Image, Graphics and Signal Processing 12.2 (2020): 30.
33. Erwin, Erwin. "Similarity-Improving Retinal Image Quality Using the Contrast Stretching, Histogram Equalization, and CLAHE Methods with Median Filters." (2020).
34. Hussien, Nadheer Younus, Rasha O. Mahmoud, and Hala Helmi Zayed. "Deep Learning on Digital Image Splicing Detection Using CFA Artifacts." International Journal of Sociotechnology and Knowledge Development (IJSKD) 12.2 (2020): 31-44.
35. Velmurugan, S., T. S. Subashini, and M. S. Prashanth. "Dissecting the Literature for studying various Approaches to Copy Move Forgery Detection." IJAST 29.04 (2020): 6416-6438.
36. Meena, Kunj Bihari, and Vipin Tyagi. "A Deep Learning based Method for Image Splicing Detection." Journal of Physics: Conference Series. Vol. 1714. No. 1. IOP Publishing, 2021.