Copy-Move Forgery Detection Based on Euclidean Distance and Texture Feature Analysis

Ashutosh Kumar[a], Neha Janu[b]*

[a]*Department of Computer Science & Engineering, JECRC University, Jaipur, India*
[b]*Departtment of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, Rajasthan, India*

Abstract

Digital images are important part of our life. Copy and Move forgery detection techniques are designed to detect edited part of the image. The copy and move forgery techniques are based on the feature detection and matching. The techniques which are designed so far use the Euclidean distance concept for feature matching. The feature detection techniques which are much popular like Haar transformation are used for feature extraction. In this research, the PCA algorithm is used for the simplification of features which are extracted with Haar transformation. The GLCM algorithm is used for texture feature analysis of input image. In the end, Euclidean distance is used for feature matching and mismatched features are marked as forgery. The proposed approach is implemented in MALTAB and results are analyzed in terms of accuracy.

Keywords: GLCM; PCA; Haar; Euclidean Distance.

1. Introduction

The technique which is used to improve raw images obtained from the cameras equipped on satellites, space probe and aircrafts is called image processing. These images are used to capture a number of usual ruckuses of time for various applications. In image processing approach, massive growth has been seen in the last few years. The image processing is one of the frequently used applications [1]. This approach is utilized to improve the visual form of pictures. In image processing, the images are generated to measure useful information extracted from these images. The visual image along with analog image processing can be obtained with its importance using this technique [2]. In this work, the various common approaches implemented to the images are offered. The image is obtained through imaging procedure. Thus, digital image processing is recognized as a complete procedure that is applied on images. This method makes visual and analog image processing possible. The images can be developed using various fields like computer graphics in image processing approach. The images are modified and improved using image processing technique. The vision of computer is used to analyze images [3]. The separated images are available in a photo. These separated images are called important regions. An image normally includes collection of objects. This collection is the base for an area. A lot of growth has been seen in the image processing technology in the last few years. The large numbers of images can be captured using advanced digital cameras. These cameras capture images with no noticeable traces [4]. Nowadays, the automatic forgery detection algorithms are getting quite popular due to their ability to driven the reliability of the object image [5]. A passive forgery detection algorithm is needed that does not require any

* Corresponding author
E-mail address: nehajanu@skit.ac.in

ARK: https://n2t.net/ark:/47543/JISCOM2022.v3i1.a28

previous information related to the image content or any defending techniques like watermarks. The image manipulation method is not a novel method but a sub division of image acquisition. In the past, manual techniques were used to identify the image forgery. The growth of technology and expansion in database storage started the storage of data in the digitized form [6]. This factor raised security challenges. Therefore, the documents became more prone to digital doctrine. The digital forgery methods are discovered by the Digital Images Forensics (DIF). This approach is identified as the shield of images and security methods and regains the consistency of images. Some important features like addition, alteration or content removal define the changes within an image. The images get changed without leaving any visible mark. Various techniques are used for image forgery [7]. The digital image forgery can be separated into three main groups such as Copy-Move forgery, Image splicing, and Image resampling with regards to such techniques that are used to generate fake images. The Copy-Move Forgery is a commonly used image manipulation technique because of its easiness and effectiveness. This technique is widely utilized in various applications due to the advent of technology [8]. In this technique, some part of the image gets copied and pasted on some other part in the same image to conceal some important information. Image splicing generates fake images using one or more images. In case of incorrect splicing, the boundaries amid spliced parts can be imperceptible [9]. On the other hand, this technique generates interruptions in high order Fourier statistics. Thus, these insights can be utilized as a part of individual forgery. In this technique, two different images are combined as a solo image [10]. The geometric alterations such as rotation, scaling, stretching, skewing, flipping etc are applied on every selected part to develop an effective and amazing false image. The interpolation step is crucial in this process. This step initiates non-negligible statistical changes [11]. Within the image, some specific episodic associations are triggered by the resampling. Copy-move forgery is a commonly used image tampering technique. In this technique, some part of the image is cut, copied and pasted on some other image to hide redundant regions of the image. This technique has gained a lot of popularity due to its simplicity and effectiveness. This technique is broadly used in many applications due to the advent of technology [12]. The merits and demerits of this technique specifically depend upon its way of use. This technique generates false images. The generated forged images are further used to hide real data. The textured regions are used as similar color and noise difference features to perform copy move forgery [13]. The human eye is not capable to notice these types of alterations in image statistical properties. The burring is generally used close to the edge of changed region to minimize recklessness among the real and pasted part. This tampering also involves the overlapping of one object within an image by some other object of the same image [14].

2. Literature Review

Geetika Gupta, et.al (2017) proposed a new approach to identify copy move forgery. The proposed approach did not need any information about original image. Using the grayscale image, the overlapping blocks were introduced initially. In addition, the hybrid methodologies were used for feature extraction. These techniques integrated PCA and histogram of oriented gradients [15]. Lastly, the features were sorted in lexicographic way which made the matching of simulated regions trouble-free. The evaluation results discovered that the proposed approach showed better results and improved security for two unlike attacks. Also, the obtained outcomes were highly efficient in terms of different parameters like precision, recall and accuracy.

Yong Yew Yeap, et.al (2018) reviewed copy move technique. This technique used passive forgery detection method to corrupt images. The copy move forgery detection (CMFD) was a category of passive forgery detection approach. A procedure named rotated Binary Robust Independent Elementary Feature was utilized to extract features [16]. In this study, a new featuring method was proposed. The proposed CMFD technique was evaluated in this work. This technique processed images from various geometrical intrusions. The proposed approach depicted the accuracy level of 84.33% and 82.79% correspondingly. Two different databases were used for assessment. Thus, the proposed approach demonstrated True Positive Rate above 91% for degraded images using forgery detection.

Dhanya R, et.al (2017) reviewed that the Image forgery detection technique became very popular in forensic science field due to the expansion of image processing approach. A brief review was provided on the copy-move forgery discovery technique in this work. This work presented all accessible techniques with their proper stages. These techniques were not used extensively due to confines of earlier approaches. There was the scope of more enhancements

in these approaches [17]. The key purpose of this work was to remove the former restrictions of accessible techniques with the help of proposed technique. The experimental outcomes indicated that the proposed technique was able to design the low-cost image forensic applications.

Yue Wu, et.al (2018) projected a most recent deep neural network to recognize and predict the forgery masks in a simple way. The main aim of proposed technique was to identify the copy-move forgery. A convolutional neural network was proposed in this work [18]. The proposed technique was applied to extract the features of matching blocks. This technique calculated self-correlations in different blocks. This system was utilized to optimize the loss occurred in the rebuilding of forgery surface. The simulations performed on different features and matching systems revealed that the proposed approach showed superior results as compared to earlier approaches. The proposed technique showed high probability to protect image data from anonymous intrusions.

Hanieh Shabanian, et.al (2017) proposed a novel block-based approach to detect copy-move forgery from digital pictures [19]. The originality of the proposed technique lied in the utilization of structural similarity index. This similarity index was used as a technique of similarity matching stage. Hence, the proposed approach did not need feature extraction. The feature extraction process could provide support in the lessening of time-consuming problem. In view of that, the important requirement of proposed scheme occurred in the ease of calculation and evaluation. Several tests were conducted to demonstrate the effectiveness of recommended approach. The strength and responsiveness of proposed approach was evaluated alongside some post-processing tasks.

Rahul Dixit, et.al (2017) proposed a novel approach to partition images into overlapping blocks of finite size. The frequency domain and the statistical features of an image were considered by the proposed approach [20]. In this work, two parameters named as DA and FPR were utilized to test the efficiency of proposed technique. Using these parameters, the performance of proposed approach could be compared with other existing approaches. The tested outcomes depicted that the proposed approach gave superior as compared to other existing approaches. The proposed approach provided improved accuracy and false positive rate.

3. Research Methodology

This research study is based on the PCA algorithm. This algorithm is used to find different areas in a digital data. The PCA algorithm marks copied part with black color. PCA is a multivariate algorithm. This algorithm analyzes data table. This data table depicts various related quantitatively dependent variables. The main aim of this algorithm is to extract useful information from the table. The extracted information represents new orthogonal variables. These variables called principal components.

In this work, the similarity patterns of observations and the variables as points in maps are displayed. The data is centered mainly regarding every variable when a known data matrix includes p variables and n samples. The data exists in the center on the source of principal components. This phenomenon does not affect the spatial relations of data or the variances present with the variables. The initial principal component 〖(Y〗_1) is applied by the linear combination of variables X1, X2, ...,Xp. This combination id described below:

$$Y\_1=a\_11\ X\_1+a\_12\ X\_2+\cdots+a\_1p\ X\_p \quad \ldots (1)$$

This combination as matrix notation can be specified as below:

$$Y\_1=a\_1\text{^}T\ X \quad \ldots (2)$$

The preliminary principal component is computed to find the highest possible variance in the data set. The variance of Y_1 can be created by choosing the large values for weights a_11,a_12,…a_1p. The weights are calculated carefully to make sum of squares equal to 1, in order to avoid such condition.

$$a\_11\text{^}2+a\_12\text{^}2+\cdots+a\_1p\text{^}2=1 \quad \ldots (3)$$

In the similar manner, the second principal component is calculated to avoid correlations towards the initial principal component. The next greatest variance uses this second principal component.

$Y_2=a_{21} X_1+a_{22} X_2+\cdots+a_{2p} X_p$ … (4)

This procedure continues till the calculation of p principal components. These components are equivalent to the real number of variables. Equal values are attained for the sum of variances of all principal components and the sum of variances of all variables in this point. Thus, the changes occurring in all original variables to the principal components can be indicated as:

$Y=XA$ … (5)

In this work, the GLCM algorithm is used to find out textual features of an input image. Within the image, the area of copy-move forgery is detected using these known features. The statistical texture analysis is used to compute texture features equivalent to each other. The statistics is categorized into first-order, second-order and higher order as per the accessible intensity points within every grouping. Using GLCM algorithm, the second order statistical texture features can be extracted without difficulty. This algorithm gives information about the location of pixels having alike gray level values. A matrix containing equivalent number of rows, columns and gray levels within an image is termed as GLCM.

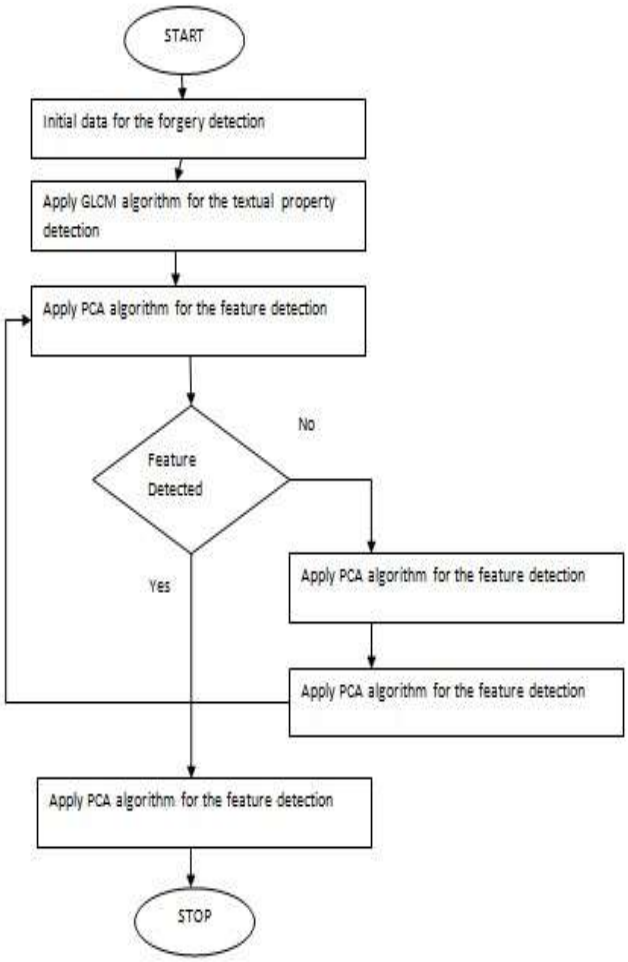

Fig. 1. Proposed Flowchart

4. Experimental Results

The proposed research is implemented in MATLAB and results are evaluated by comparing proposed and existing techniques in terms of several performance parameters.

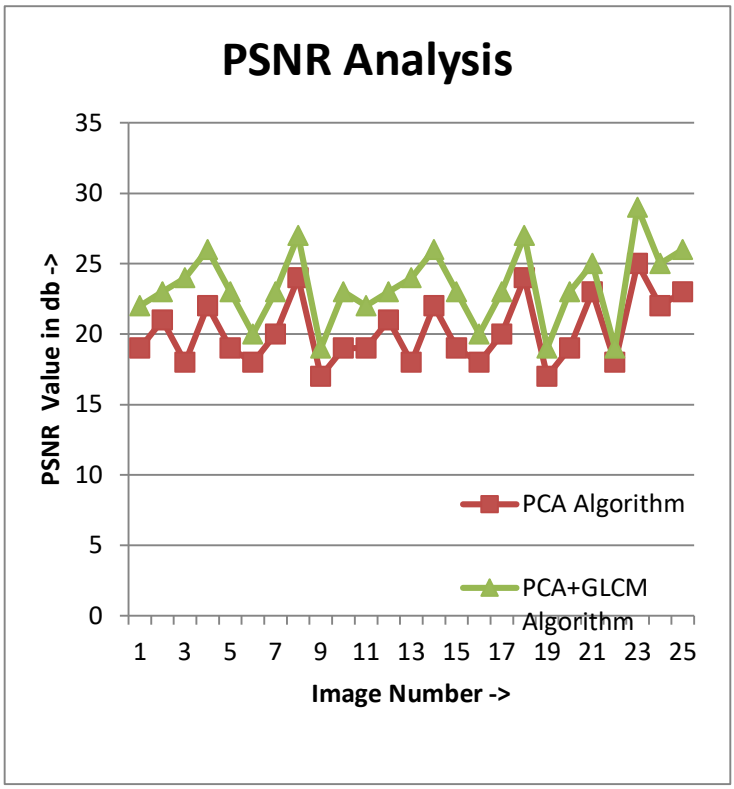

Fig. 2. PSNR Comparison

Figure 2 reveals that PCA algorithm and PCA algorithm along with GLCM are implemented to detect copy-move forgery. The PCA with GLCM algorithm gives better PSNR value as compared to the PCA algorithm

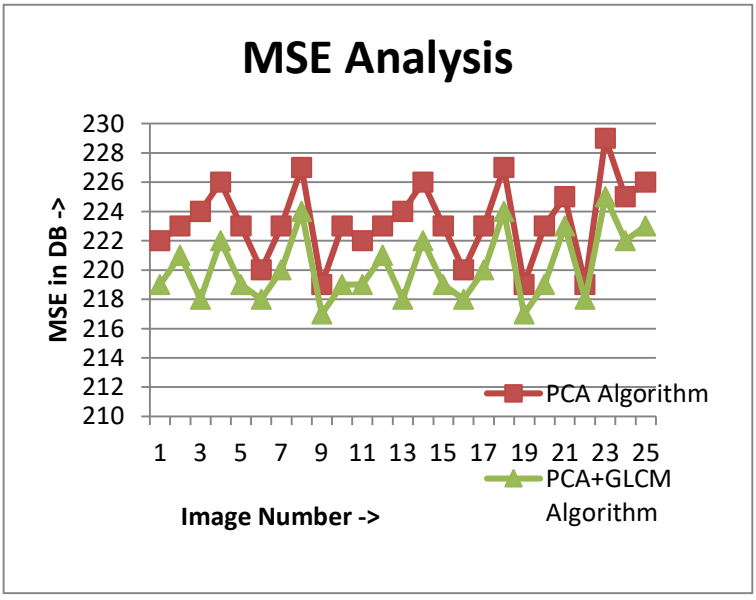

Fig. 3. MSE Comparison

The figure 3 shows that the performance of PCA algorithm and GLCM with PCA algorithm is analyzed by comparing them in terms of MSE value. The PCA algorithm gives better MSE value than GLCM with PCA algorithm as per the analysis.

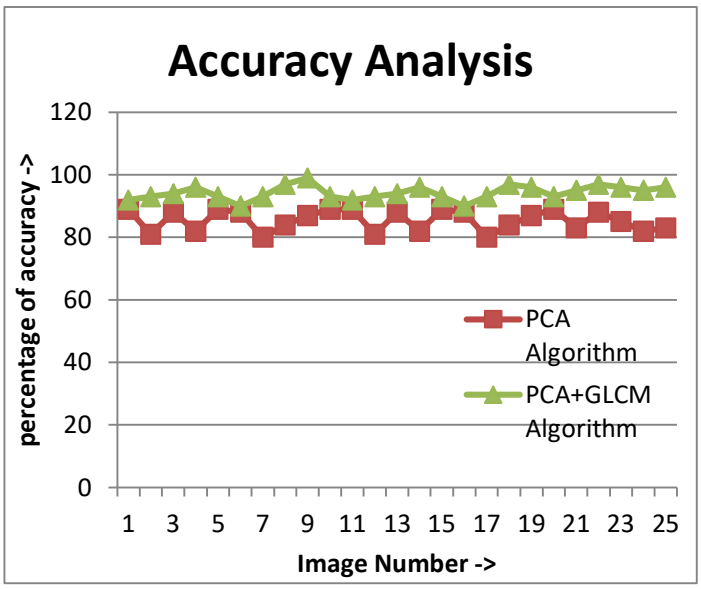

Fig. 4. Accuracy Comparison

The figure 4 shows that the performance of PCA algorithm and GLCM with PCA algorithm is analyzed by comparing them in terms of accuracy. The proposed approach shows better accuracy rate than the earlier approach as per the analysis.

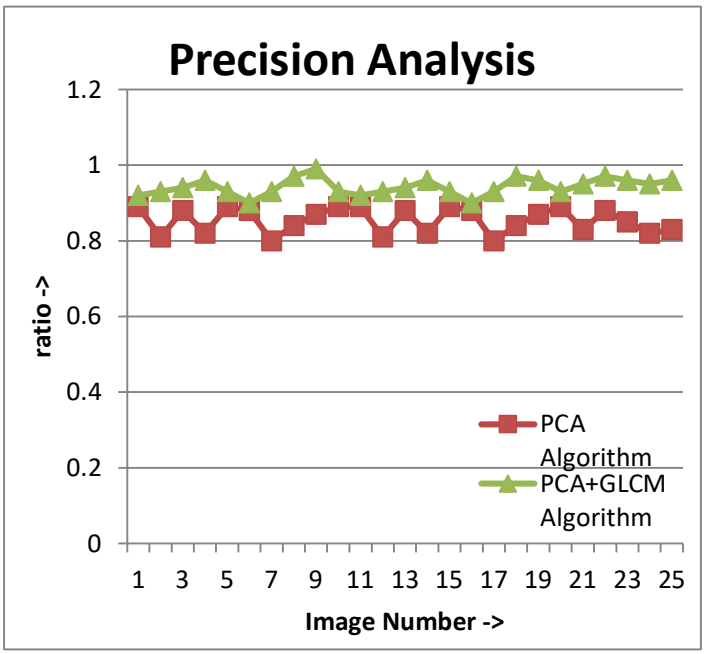

Fig. 5. Precision Comparison

The figure 5 shows that the performance of PCA algorithm and GLCM with PCA algorithm is analyzed by comparing them in terms of precision. The proposed approach shows better precision value than the earlier approach as per the analysis.

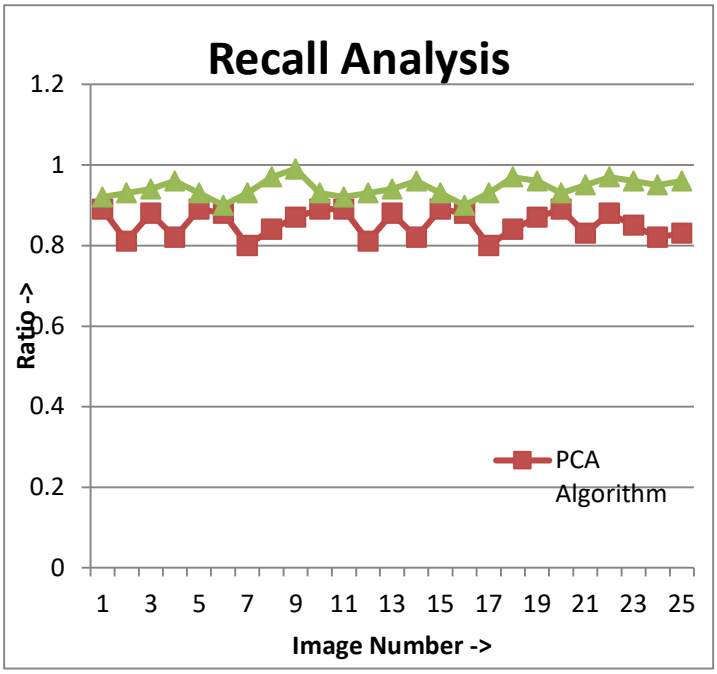

Fig. 6. Recall Comparison

The figure 6 shows that the performance of PCA algorithm and GLCM with PCA algorithm is analyzed by comparing them in terms of recall value. The proposed approach shows better recall value than the earlier approach as per the analysis.

5. Conclusion

The data collected in the form of images is processed by the image processing approach. The forgery detection technique is used to identify interfered parts of the input image. The existing approach used PCA algorithm to identify forgery. The PCA algorithm is known as Principle Component Analysis. The forged part of the image is detected using this algorithm. In this work, the GLCM algorithm is applied along with the PCA algorithm to identify forgery. The proposed technique is a grey-level co-occurrence matrix. This algorithm detects the textural properties of the image by calculating co-occurrence matrix. The GLCM algorithm along with PCA algorithm marks all forged parts on the image. The MATLAB tool is used to simulate proposed and existing algorithms. It is analyzed that proposed approach has high PSNR value and low MSE value.

References

[1] L. Kang, and X.-P. Cheng, "Copy-move forgery detection in digital image," in 3rd International Congress on Image and Signal Processing (CISP 2010), IEEE Computer Society, 2010, pp. 241921.

[2] Z. Lin et al., "Fast, automatic and fine-grained tampered JPEG image detection via DCTcoefficient analysis", Pattern Recogn., Vol. 42, pp. 2492250, 2009.

[3] Bayram S., Avcibas I., Sankur, and B. Memon N., "Image manipulation detection," Journal of Electronic Imaging – October - December 2006 – Volume 15, Issue 4, 041102 (17 pages), vol. 15(4), 2006.

[4] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.

[5] M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.

[6] M.Wu A. Swaminathan and K. J. Ray Liu, "Image tampering identification using blind deconvolution," Proc. IEEE ICIP, 2006.

[7] Sencar H. T. Memon N. Sutcu Y., Coskun B., "Tamper detection based on regularity of wavelet transform coefficients," Proc. ICIP, International Conference on Image Processing, 2007.

[8] J. Fridrich, D. Soukal, and J. Luk, "Detection of copymove forgery in digital images," Proc. Digital Forensic Research Workshop, Cleveland, OH, August 2003.

[9] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Technical Report, TR2004-515, Dartmouth College, Computer Science, 2004.

[10] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, 1991.

[11] Qiong Tu Dan Sun Shaojie Li, Guohui Wu, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on dwt and svd," ICME, 2007.

[12] Weiqi Luo, Jiwu Huang, and Guoping Qiu, "Robust detection of region-duplication forgery in digital image," in ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition, Washington, DC, USA, 2006, pp. 746–749, IEEE Computer Society.

[13] Sevinc Bayram, Taha Sencar, and Nasir Memon, "An efficient and robust method for detecting copy-move forgery," submitted to ICASSP 2009, 2009.

[14] J. A. Bloom I. J. Cox M. L. Miller C. Y. Lin, M.Wu and Y. M. Lui, "Rotation, scale,and translation resilient watermarking for images," IEEE Trans. Image Processing, vol. 10, pp. 767–782, 2001

[15] Geetika Gupta, Akshay Girdhar, "A ROBUST PASSIVE METHOD FOR DETECTION OF COPY-MOVE FORGERY IN IMAGES", 2017, IEEE

[16] Yong Yew Yeap, U. U. Sheikh, Ab Al-Hadi Ab Rahman, "Image Forensic for Digital Image Copy Move Forgery Detection", 2018 IEEE 14th International Colloquium on Signal Processing & its Applications (CSPA 2018)

[17] Dhanya R1, R Kalai Selvi, "A State of the Art Review on Copy Move Forgery Detection Techniques", Proceedings of 2017 IEEE International Conference on Circuits and Systems (ICCS 2017)

[18] Yue Wu, Wael Abd-Almageed, and Prem Natarajan, "Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network", 2018 IEEE Winter Conference on Applications of Computer Vision

[19] Hanieh Shabanian, Farshad Mashhadi, "A New Approach for Detecting Copy-Move Forgery in Digital Images", 2017, IEEE

[20] Rahul Dixit, Ruchira Naskar and Aditi Sahoo, "Copy–Move Forgery Detection Exploiting Statistical Image Features", IEEE WiSPNET 2017

[21] Neha Janu, Pratistha Mathur, "Performance Analysis of Feature Extraction Techniques for Facial Expression Recognition", International journal on Computer Applications, ISSN No. 0975 –8887, Volume-166, Issue-1, May 2017.

[22] Janu Neha, Pratistha Mathur, "Performance analysis of frequency domain based feature extraction techniques for facial expression recognition." In 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, 2017, pp. 591-594. IEEE, 2017.