International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

Copy-Move Forgery Detection using Discrete Wavelet Transform (DWT) Method

Avleen kour[1], Dr. Vibhakar mansotra[1]

[1]M. Tech Scholar, University of Jammu, Jammu and Kashmir, INDIA
[2]Professor, Dean, University of Jammu, Jammu and Kashmir, INDIA

Abstract :- *A technique named forgery detection is used for detecting alterations from the image. This approach comprises several methods such as properties analysis, classification and so on. This research study relies on the recognition of copy-move forgery. In copy-move forgery, copied part of image which moved to other place is detected and marked. In the earlier work, the PCA algorithm is implemented for detecting forgery. The PCA algorithm will mark the principle component analysis for incompatible pixels from the picture. The GLCM algorithm is applied with the PCA algorithm in this research study for detecting forgery. The proposed algorithm is executed in MATLAB and outcomes are scrutinized on the basis of PSNR and MSE values. It is scrutinized that the proposed algorithm gives good performance in comparison with earlier algorithm.*

KEY WORDS: **DWT, PCA, GLCM**

Introduction

Image Processing is defined as an approach used to enhance the unprocessed pictures captured by satellites, space probe and aircrafts. These pictures are seized for capturing a variety of usual commotion of time for different applications. In the last four to five decades, a lot of improvements have been made in image processing approach. Various applications like military areas, spaceships, etc. require the extraction of useful information through image processing [1]. Due to the accessibility of prevailing personal workstation, big range memory devices and graphics software, the technique of picture handling have become popular in different regions. The image processing is most commonly used application which is used to enhance the visual appearance of images. In this approach, pictures are created for measurement of important information which can be extracted from them. The visual plus analog image processing can be provided along with its significance. Several general approaches are applied to images which are presented here. Imaging process is used for image acquisition [2]. Therefore, digital image processing is identified as an absolute process that is to be carried out. This technique makes optical and analog image processing feasible. In image processing, the images can be generated with the help of several fields such as computer graphics. The image processing approach modifies and improves the images. The images are analyzed by means of computer vision [3]. The divided pictures are accessible in a picture and are identified as significant areas. An image generally contains compilation of objects which is the foundation for a region. The technology of image processing is growing rapidly. The advancement of digital cameras has made possible the generation of large amount of images without any observable mark. Thus, automatic forgery detection algorithms are in a great demand as they are able to determine the trustworthiness of a candidate picture [4]. A passive forgery detection algorithm is required which does not need any prior information regarding the content of picture. This algorithm also has no information about protecting techniques like watermark. A technique named image manipulation is not new. This technique is a sub part of photograph capturing. This technique is used during picture capturing. The image tampering was detected manually in part years. These days, data is being stored in digital form due to the expansion of technology and enhancement in database storage. This is turn increases security related issues. The security issues make documents further prone to digital doctoring [5]. Digital Images Forensics (DIF) is behind the exploration of digital forgery methods. Digital forgery method preserves images and safety methodologies. This approach restores the reliability of pictures. Addition, transformation or removals of content are some essential features that describe the variation inside an image. The alteration is carried out without leaving any noticeable trace. The image may be forged using different techniques. Copy-Move forgery, Image splicing, and Image resampling are the three classes in which digital image forgery can be divided with regards to the techniques utilized to create fake pictures. Due to the ease and efficiency, Copy-Move Forgery is identified as one of the most common interfering method. This method is extensively used in several applications because of the expansion of technology [6]. A segment of picture is copied and pasted to some other region in the similar picture to hide some significant information in this tampering. The method

which is used to generate false images using several pictures is called image splicing. The edges between spliced areas can be optically invisible if splicing is carried out accurately [7]. However, this phenomenon creates disturbance in high order Fourier statistics. All chosen regions go through geometric alterations such as rotation, scaling, stretching, skewing, flipping etc for creating an efficient and remarkable fake picture. In this procedure, the interpolation step is imperative. This step introduces non-negligible statistical alterations. Copy-move or region duplication forgery is the most frequent image interfering approach [8]. In this technique, some fraction of picture is cut or copied and pasted on some other picture for concealing unrequited segments of picture. Due to the ease and efficiency, Copy-Move Forgery is identified as one of the most common interfering method. Due to the expansion of technology; this method is extensively used in numerous applications. There are two wider classes in which image forgery is classified. Image tampering is the preliminary category of picture forgery which selects some particular region within a picture. In this procedure, some chosen is copied and pasted into some other picture. This technique conceals information of some specific picture [9]. The second category takes two or more images. This class copies and paste information on that image which is chosen for forging. Copy-Create Image Forgery is the other name given to this type of tampering. This procedure generates an integrated result in the last through the integration of various pictures.

Literature Review

Geetika Gupta, et.al (2017) projected a new approach for the uncovering of CMFD falsification. The proposed approach did not need any information regarding actual image. From the grayscale image, the overlapping blocks are commenced primarily [10]. This investigate study was applied on a precise existing and recently projected technique for comparing their performances. The comparative outcomes analyzed that the utilization of proposed offset threshold value provided help in the minimization of fake matches which was the major concern of earlier approach. The evaluation outcomes revealed that the proposed approach showed improved results and improved security for two different attacks. Moreover, the obtained outcomes were highly efficient in terms of different parameters like precision, recall and accuracy.

Yong Yew Yeap, et.al (2018) presented a review of copy move technique. In this technique, images were corrupted using passive forgery detection. The passive forgery detection approach was also identified as copy move forgery detection (CMFD). Due to the quickening of segmented test, the oriented features were presented in the CMFD method [11]. In this study, a novel featuring technique was proposed. In this study, the proposed CMFD technique was assessed. In this technique, images were processed from different geometrical intrusions. The proposed approach showed accuracy rate of 84.33% and 82.79% respectively. For evaluation purpose, two different databases were used. Thus, the proposed approach showed True Positive Rate of more than 91% for corrupted pictures by means of the forgery detection.

Dhanya R, et.al (2017) stated that the Image forgery detection technique played an important role in forensic science domain because of the advancement of image processing approach. In this study, a concise review was presented on the copy-move forgery finding technique. In this study, all existing techniques were presented with their suitable phases. Due to limitations of existing techniques, these techniques were not used extensively. These techniques required more improvements [12]. The main objective of this study was the elimination of earlier limitations of existing techniques using proposed approach. The tested results demonstrated that the proposed technique was extremely proficient in inexpensive design of image forensic applications.

Yue Wu, et.al (2018) projected a latest deep neural network for the easy recognition and prediction of forgery masks. The proposed approach for detect the copy-move falsification. In this study, a convolutional neural network was proposed [13]. The proposed approach was used for the extraction of block-like features. In this approach, self-correlations were computed in different blocks. The proposed approach used a point-wise feature extractor for locating matching points. A forgery mask was constructed again by using a deconvolutional network. On the basis of different features and matching systems, the simulation outcomes revealed that the proposed approach provided more help in the attainment of better results as compared to earlier techniques. The proposed method showed high feasibility rate for protecting image data from unidentified attacks.

Hanieh Shabanian, et.al (2017) stated that copy-move forgery technique was used for the manipulation of digital pictures. In this technique, the regions of same pictures were copied. A detection procedure called forgery detection was utilized for identifying the tampered regions. Novel block-based approach was proposed. The proposed approach used a structural similarity index system in the form of a similarity matching step [14]. The proposed approach could be used to minimize the issue of time consumption which in turn abolished the need of feature extraction process. The proposed technique used

important specification for making calculation and analysis easier. The tested results demonstrated that the proposed approach had improved effectiveness and sensitivity.

Rahul Dixit, et.al (2017) proposed a new approach for splitting images into overlapping blocks of fixed size. The proposed approach considered frequency domain and the statistical features of an image beside it [15]. In this study, two matrices called DA and FPR were used for the testing of proposed approach. With the help of these matrices, the performance of proposed approach could be compared with other accessible algorithms. The experimental results demonstrated that the proposed approach showed better performance in comparison with other existing approaches. The proposed approach showed better accuracy and false positive rate.

Research Methodology

This examination relies on the PCA method. This technique is employed for finding the dissimilar areas in a digital data. The copied region is marked with black color with the help of PCA algorithm, it is a multivariate manner which is used to analyze data table. This data table represents several interrelated quantitatively dependent variables. The major purpose of this approach is the extraction of important information from the table for the representation of novel orthogonal variables. These variables are known as principal components.

The patterns of similarity of observations and the variables in the form of points within maps are displayed here. The data is centered primarily with respect to each variable when a given data matrix contains p variables and n samples. On the origin of principal components, the data occurs in the middle which however does not influence the spatial relations of data or the variances present along the variables. The initial principal component (Y_1) is specified through the linear combination of variables X_1, X_2, ...,X_p which is given below:

$$Y_1 = a_{11}X_1 + a_{12}X_2 + \cdots + a_{1p}X_p \quad \ldots (1)$$

In the form of matrix notation, it can be specified as:

$$Y_1 = a_1^T X \quad \ldots (2)$$

The initial principal component is calculated for finding the greatest possible variance within the data set. Selecting large values for weights$a_{11}, a_{12}, \ldots a_{1p}$, the variance of Y_1 can be made. The weights are computed with the constraint such that the sum of squares is 1, to prevent such condition.

$$a_{11}^2 + a_{12}^2 + \cdots + a_{1p}^2 = 1 \quad \ldots (3)$$

The second principal component is computed in same way as no correlation occurs towards the initial principal component. The next highest variance utilizes this second principal component.

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

This process remains continue till the computation of p principal components. These components are equal to the original number of variables. Equivalent values are obtained for the sum of variances of all principal components and the sum of variances of all variables in this point. Therefore, the alterations of all original variables to the principal components can be demonstrated as:

$$Y = XA \quad \ldots (5)$$

In this research study, the textual features of an input image are detected with the help of GLCM algorithm. By using these identified features, the region of copy-move forgery is detected from the image. The texture features are calculated at particular positions corresponding to each other using statistical texture analysis. On the basis of available intensity points within each combination, the statistics is classified in first-order, second-order and higher order. The second order statistical texture features can be extracted easily with the help of GLCM algorithm. The GLCM algorithm provides information related to the positions of pixels that include similar gray level values. A matrix which comprises equal number of rows, columns and gray levels in an image is called GLCM.

The relative frequency through which two pixels are separated at distance d, for which specific angle (θ) defines the direction, i and j define the intensities of both the pixels, is defined as P(i, j | d, θ).

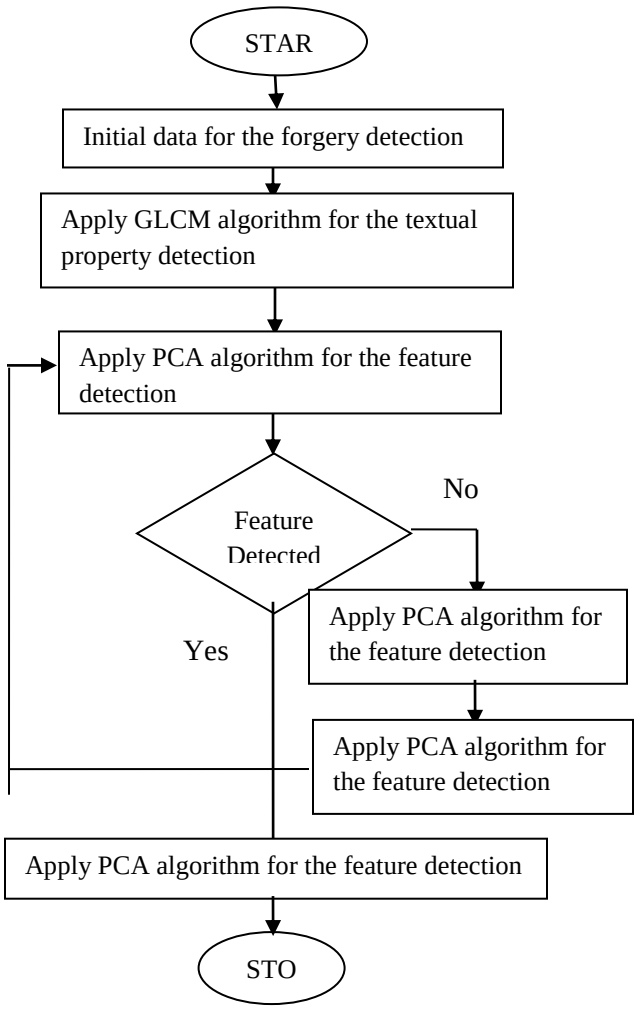

Fig 1: Proposed Methodology for CMFD

Experimental Results

The proposed research is implemented in MATLAB and the results are evaluated by comparing proposed and existing methods with respect to certain performance measures.

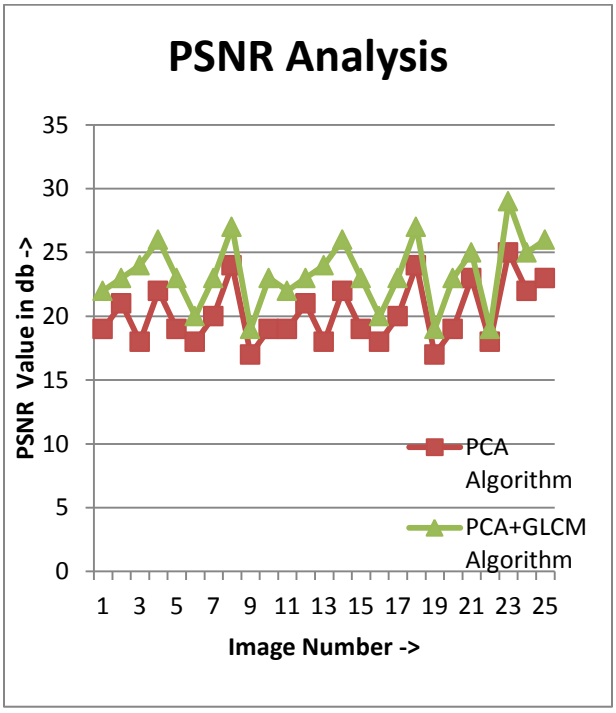

Fig 2: PSNR Comparison

The PCA algorithm and PCA algorithm in conjunction with GLCM are applied for the copy-move forgery recognition as depicted by the figure 2. The PCA with GLCM algorithm comprises higher PSNR value in comparison with PCA algorithm.

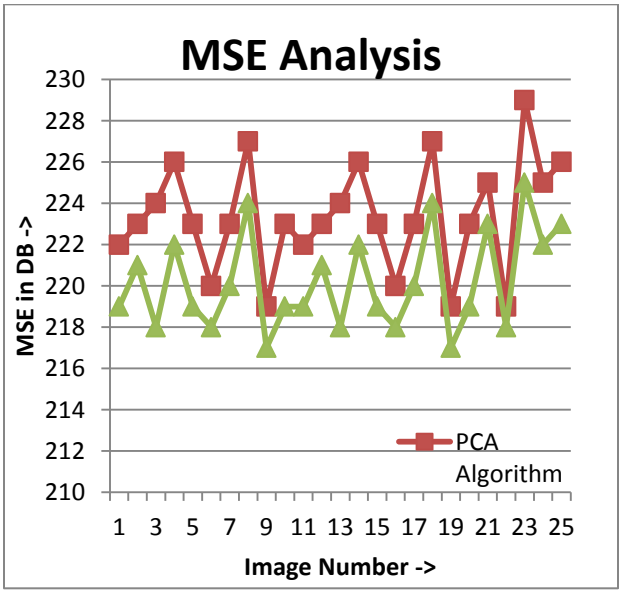

Fig 3: MSE Comparison

For performance analysis, the MSE value of PCA and GLCM with PCA algorithm is compared as depicted by figure 3. It is analyzed that MSE value of GLCM with PCA algorithm is low as compared to PCA algorithm.

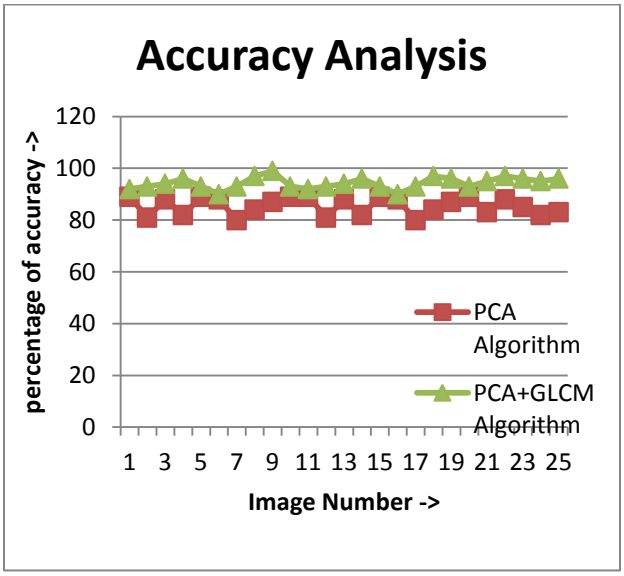

Figure 4: Accuracy Comparison

For performance analysis, the accuracy value of proposed and existing algorithm is compared as depicted by the figure 4. It is examined that accurateness rate of projected methodology is high in comparison with the presented methodologies.

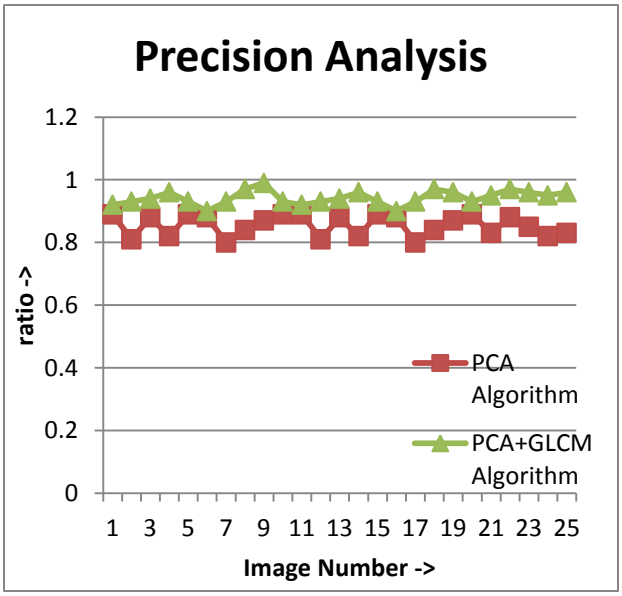

Figure 5: Precision Comparison

For performance analysis, the precision value of existing and proposed algorithm is compared as demonstrated by the figure 5. The precision rate of projected methodology is high as compared to presented algorithm.

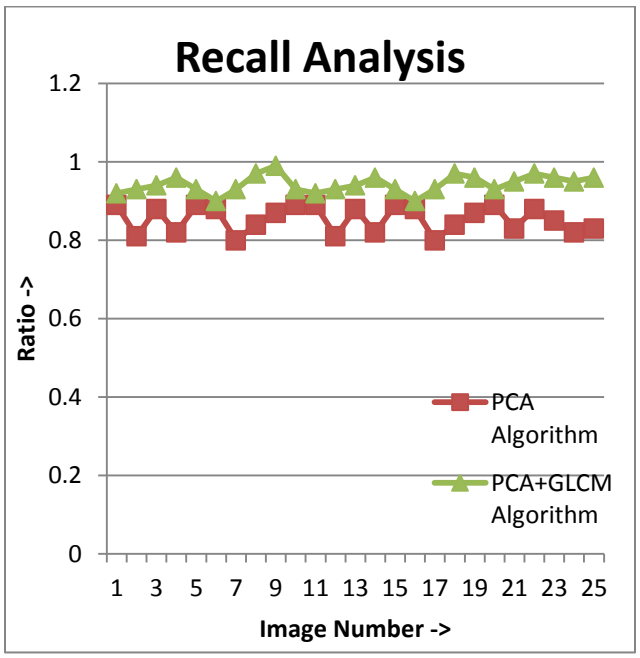

Figure 6: Recall Comparison

For performance analysis, the recall rate of projected as well as presented methodology is measured as depicted by the figure 6. It is scrutinized that recall value of projected methodology is high as in contrast with presented methodology.

Conclusion

Image processing approach is used to process data accumulated as picture elements. The tampered regions of input pictures can be detected with the help of forgery detection approach. In the earlier approach, PCA algorithm is implemented for the forgery recognition. The PCA algorithm stands for Principle Component Analysis. The tampered region of picture is detected with the help of this algorithm. GLCM algorithm is implemented in conjunction with PCA algorithm in this investigative study to detect forgery. The projected method is grey-level co-occurrence matrix. In this algorithm, the textural properties of picture are identified by computing co-occurrence matrix. The GLCM technique is described with PCA methodology which marks all fake pixels on the picture. The proposed and existing methods are simulated using MATLAB tool. It is scrutinized that proposed approach comprises high PSNR 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] Geetika Gupta, Akshay Girdhar, "A ROBUST PASSIVE METHOD FOR DETECTION OF COPY-MOVE FORGERY IN IMAGES", 2017, IEEE

[11] 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)

[12] 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)

[13] 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

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

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