Indian Journal of Science and Technology, Vol 9(35), DOI: 10.17485/ijst/2016/v9i35/98605, September 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Image Forgery Detection using SIFT and PCA Classifiers for Panchromatic Images

Navneet Kaur* and Nitish Mahajan

Chandigarh University, Gharuan - 140413, Punjab, India;
navneetkaur2619@gmail.com, nitish2mahajan@gmail.com

Abstract

Objectives: The image forgery detection is the technique in which pixels are marked in the image, which are not similar to other pixels of the images. The Principal Component Analysis (PCA) is the classification of neural networks which will analyze each pixel of the image and classify pixels according to pixel type. **Method:** The PCA algorithm takes training and trained dataset as input and drive new values according to input image. In the paper improvement in the PCA algorithm with usage of Scale-Invariant-Feature-Transform algorithm (SIFT Algorithm), is proposed for image-forgery. The SIFT algorithm is the algorithm which analyze each pixel of the image and define type of pixels in the image. The output of the SIFT algorithm is given as input to PCA algorithm for data classification. The PCA algorithm will classify the data according to SIFT algorithm output. **Findings:** The results demonstrate that the proposed algorithm executes well in terms of "Peak Signal-to-Noise Ratio" (PSNR), "Mean-Square-Error" (MSE), fault detection rate and accuracy value.

Keywords: Forgery Detection, MSE, PCA, PSNR, SIFT

1. Introduction

A digital-image is an array of real numbers shown by a finite number of bits[1]. Image processing technique is used for enhancement of raw images which are received from the sensors, cameras which are sited on satellites and aircrafts. The Region based segmentation can be defined as partitioning the image into regions[2]. Edge detection techniques have been utilized in this way as the base of another segmentation technique. The watershed transformation considers the gradient magnitude of an image as a topographic surface[3].

An image can be manipulated using various techniques of image processing like scaling, rotation, blurring, filtering and cropping. Forgery detection is required for various fields of image processing. Distinguishing forgery in digital-images is a rising examination field with essential ramifications for guaranteeing the validity of digital images[4]. After the selection of suitable classifier, existing technique extract features from the image and classify its features. At last, few forgeries like copy-move and splicing may require post-processing which include operations like localization of duplicate areas. Digital-Image-forgery-detection can be divided in two categories[5]: 1. Active approach and 2. Passive Approach. In the active-approach, digital-image requires some preprocessing like embedded watermark or signature generation at the season of creating the image and farthest point its application. Passive-approach does not require any digital signature for the authentication of the image[6]. Classification method is capable for processing a more extensive assortment of data than regression and due to this reason it is growing in popularity. There are number of classifiers available for classification techniques which are: Decision-Tree-Induction, K-Nearest Neighbors, Bayesian-Networks and Instance Based Learning. SIFT is Scale-Invariant-Feature-Transform gives motion tracking, multi-view geometry and recognition. Applications incorporate robotic mapping, image stitching, object recognition and navigation, gesture recognition, 3D-modeling, video tracking, individual identification of untamed life and match moving. SIFT algorithm is less

*Author for correspondence

time consuming algorithm and produces outcomes that are superior to the other algorithms.

2. Previous Work

In[7] proposed in this paper that there is additionally a need of environmental monitoring which should be possible through the image receivables from specific areas. The Object-based analysis is being utilized now which is another technique and can be useful to give the data required. The extensive pixel images give considerably more information which is much for informatory. The extraction of image data is utilized for spatial arranging. This data can likewise be utilized for monitoring programs. The data that is gotten can grow significantly more changes which can be useful for different fields moreover. Such changes that should be made can be watched additionally from far distances and can be overviewed every once in a while. Author in[8] proposed in this paper that image forgery is a noteworthy issue in today's time and huge test for the general public. The forgery image incorporates object evacuation, medications, object colors. In the proposed technique, image is pre-processed to the altered size. The objects are extracted from the last image and edge pixels are recognized and mapped to the first image, sensitive hash is developed for those identified regions. This future technique outflanks the current framework by precisely recognizing saliency regions, expands the affectability of the hash, decreasing hash length so that even the little area tampering can be identified correctly. Author in[9] proposed a strategy in this paper which is based on the perception that numerous preparing operations, both inside and outside securing gadgets, leave unmistakable intrinsic prints on digital images, and these intrinsic fingerprints can be recognized and utilized to check the honesty of digital data. Any change or irregularities among the assessed camera-forced fingerprints, or the nearness of new sorts of fingerprints propose that the image has experienced some sort of handling after the underlying catch, for example, tampering or steganographic embedding. Through analysis and broad test thinks about, this paper shows the adequacy of the proposed system for nonintrusive digital image criminology. Author in[10] proposed the execution of descriptors figured for nearby intrigue regions. They considered shape context, PCA-SIFT, steerable filters, complex filters, differential invariants, spin images, SIFT, minute invariants and cross-relationship for various sorts of interest regions. They additionally proposed an extension of the SIFT descriptor and demonstrate that it outflanks the principal strategy. Furthermore, it is watched that the positioning of descriptors is generally independent of interest region detector and that the SIFT based descriptors perform the best. Minutes and steerable filters demonstrate the best execution amongst the low-dimensional descriptors. Author in[11] has examined an enhanced median-filter algorithm is executed for the de-noising of exceptionally corrupted images and edge preservation. Mean, median and enhanced mean-filter is utilized for noise detection. The noise is Gaussian and impulse (salt-and-pepper) noise. An algorithm is intended to compute the PSNR and MSE. A novel strategy in light of proficient noise-detection algorithm is contemplated here for viably de-noising to a great degree corrupted images and better edges preservation. The recreation results demonstrate that the concentrated on strategy can be connected to various sorts of image and give exceptionally fulfilling results. Author in[12] proposed that present object-recognition algorithms use neighborhood features, for instance, Scale-Invariant-Feature-Transform (SIFT) and speeded up robust features (SURF), for outwardly figuring out how to perceive objects. In reality, in transmitting light, straightforward objects have the exceptional normal for mutilating the background by refraction. In the strategy they utilized a solitary shot light-field image as information and model the distortion of light-field brought about by the refractive characteristic of a straightforward object. They proposed another feature, called the light-field-distortion feature, for distinguishing a straight forward object. The proposition fuses this Light-Field-Distortion (LFD) feature to the pack of features approach for perceiving straightforward objects. They assessed its execution in research facility and real settings.

The previous work has discussed various techniques for forgery detection. The techniques use object-based analysis, image preposition technique for size variations, and usage of fingerprints has been used. The outputs for each used technique are given and the procedures are discussed. Some techniques have also used the descriptors, enhanced median filters as well as object-recognition algorithms such as SIFT, SURF etc. The various works proposed have shown their own merits and demerits in various ways.

3. PCA Classifier for Image Forgery

The image is changed over from colour to grayscale. The image is isolated into a few little sized blocks, which are broken to vectors. This is vastly improved than the Brute-Force strategy for finding the matches. The PCA technique is utilized to break the diverse blocks in an option way. PCA is fit for recognizing even minor variations because of noise and/or compression. This strategy is just for gray-scale images. Be that as it may, the strategy can be made to work for colour images also by preparing the image for every colour channel which outcomes three duplication maps. At that point PCA is connected to every map independently to recognize the forgeries. This technique has a decent proficiency in detecting Copy Move forgeries furthermore gives the less number of false-positives. In any case, the productivity drops as the piece size reduces furthermore in case the nature of image is low.

The goal of PCA is to enlarge the variance between data without considering class separation. There are distinctive methodologies proposed for a feature extraction piece. Distribution shows multidimensional raw data which is every now and again troublesome. Normally, evacuating features those are proposed to catch and address the distributions in a lower-dimensional space may unravel this mission. The PCA is frequently used for pre-processing of multi-spectral remote sensing images for the explanations behind change detection. Change, regardless, is interesting in connection to the interpretation that is used here. In remote-sensing, the change is fathomed as the technique of perceiving contrasts in the condition of an article in space by watching it at various times, for instance a vegetable canopy. In case there is no learning of what the change might be, it is not clear whether the representations in a lower-dimensional space will offer support.

4. Proposed Technique

The proposed technique is the improvement of existing technique for forgery detection. In the existing technique SIFT algorithm is used with PCA algorithm for forgery detection. The SIFT is the algorithm for properties analysis in which various different phases are used and these phases are:

- **Scale Space Extrema Detection:** This stage of filtering endeavors to recognize those locations as well as scales those are distinguishable from various perspectives of the same object/articles. This can be effectively accomplished utilizing a "scale space" function.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (1)$$

Where * is convolution operator, G(x, y, σ) is a variable-scale Gaussian, (x, y, σ) are key points and I(x, y) is the input image.

Difference of Gaussians is a method which is used for detection of stable key-point locations in the scale-space. D(x, y,σ) is calculated by computing the difference between the two images, one with scale k times the other. D(x, y,σ σ) is then given by:

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma)$$

- **Key-point Localization:** This stage endeavors to eliminate more points from the rundown of key-points by finding them that have low complexity or are inadequately localized on an edge. This is accomplished by calculating the Laplacian esteem for each key-point found in stage-1.
- **Orientation Assignment:** This step assigns an orientation which is consistent to the key-points on the basis of local image properties. The key-point descriptor can then be spoken to relative to this orientation, achieving invariance to rotation.
- **Keypoint Descriptor:** The local gradient data is also used to create key-point descriptors. The gradient information is rotated to line up with the orientation of the key-point and then weighted by a Gaussian with variance of 1.5 * key-point scale.

The key Descriptor is the last stage of SIFT algorithm which have output in terms of pixels which are not similar to that of other pixels of the image. To mark these pixels in the image for forgery classification is required which is done using PCA classifier. The PCA classifier uses two steps for classification. In the first step, it uses the orientation of the dataset. The Key descriptor of SIFT algorithm mark the points in matrixes which is of the image. The marked pixel of the dataset then sorted in the descending order and different matrices are created of the pixels

which are not similar. These different matrices pixels are then marked on the image for forgery detection.

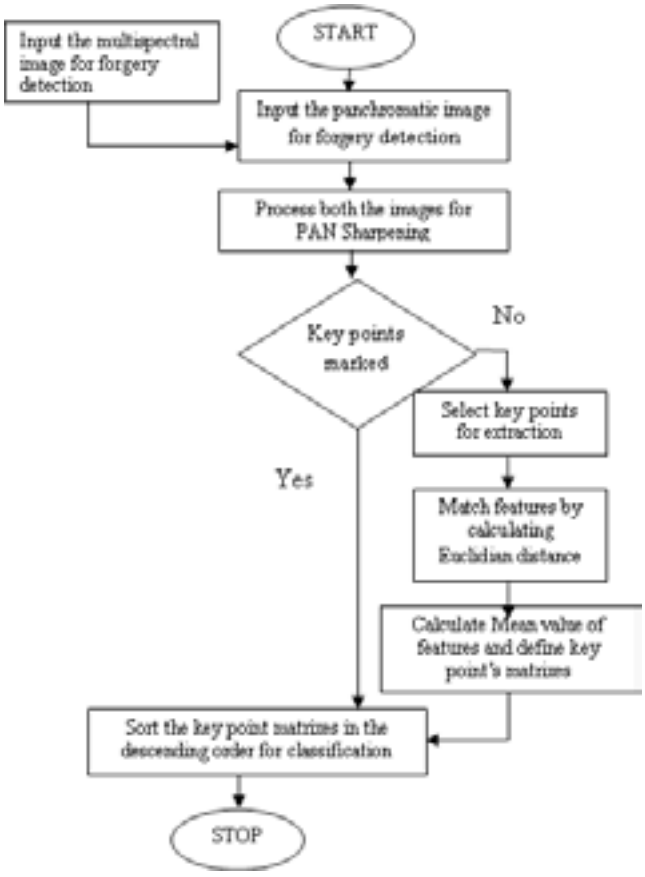

Figure 1. Proposed flowchart.

As shown in Figure 1, the proposed flowchart shows the complete working of the method. The image given as input is made to pass through certain steps. The key points are marked within the image and mean value is calculated. Euclidian distance is used for specific calculations. After the complete sorting is done, the image required is given as output and the procedure is stopped.

4.1 Experimental Graphs

Table 1. Parameter table of dataset

Parameters	Values
No of image	10
Image Format	.bmp
Dataset Size	10 Mb
Output	Marked Image with colors

As shown in Table 1, the different parameters of the image are enlisted. The parameters define the images and help in distinguishing the changes made to them.

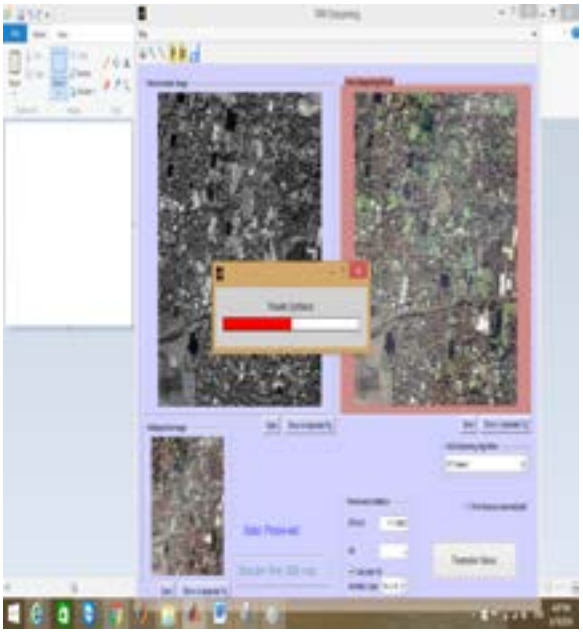

Figure 2. Apply of wavelet transformation with SIFT algorithm.

As shown in Figure 2, the algorithm is applied which is the SIFT algorithm and wavelet transformation algorithm.

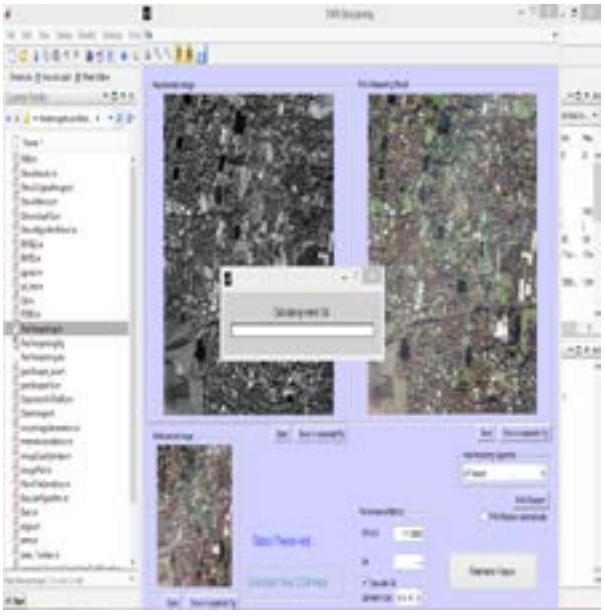

Figure 3. Calculation of Q4 matrices.

As shown in Figure 3, the algorithm is applied which is the SIFT algorithm and wavelet transformation algorithm. The SIFT algorithm will select best features from the images which are different from the image and wavelet transformation algorithm will high light that features in the image.

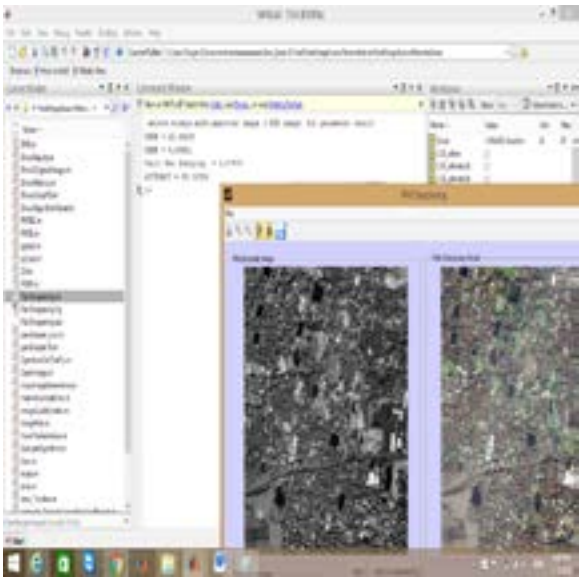

Figure 4. Display of results.

As shown in the Figure 4, after the SIFT algorithm will select best features from the images which are different from the image, the Q4 matrices are applied which will calculate features various parameters of the image like accuracy, fault detection rate and time for forgery detection. The result of the image is shown on command window in terms of PSNR, RMSE, fault detection rate and accuracy.

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20 \cdot \log_{10}[(MAX]_I) - 10 \cdot \log_{10}(MSE)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)] \quad 2$$

4.2 Comparison Table

As shown in Table 2, the different parameters of the new image are enlisted and its comparison with the already existing image is made. The parameters define the images. The existing algorithm gives certain outputs which are made to compare with the new proposed algorithm. As the results show, the new image has shown 92% of accuracy and there is a decrease in the MSE value.

Table 2. Table of comparison.

Parameter	Existing Algo	Proposed Algo
PSRN	95	115
MSE	80	55
Accuracy	81 %	92 %

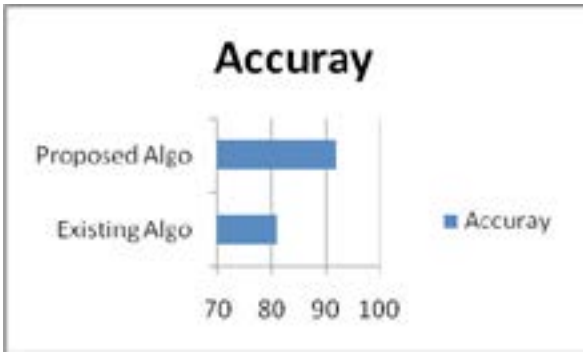

Figure 5. Accuracy comparison.

As shown in Figure 5, the different parameters of new image are compared with the already existing image is made. The parameters define the images. The existing algorithm gives certain outputs which are made to compare with the new proposed algorithm. As the results show, the new image has shown 92% of accuracy. The outputs are shown in a bar graph.

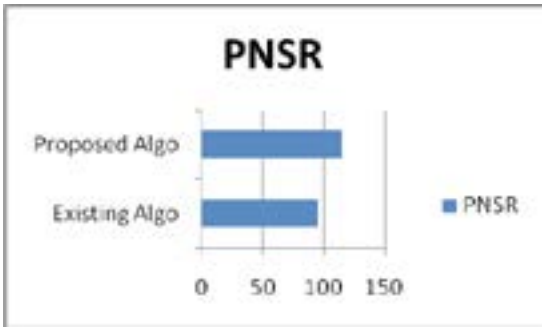

Figure 6. PSNR comparison.

As shown in Figure 6, the different parameters of new image are compared with the already existing image is made. The parameters define the images. The existing algorithm gives certain outputs which are made to com-

pare with the new proposed algorithm. The outputs are shown in a bar graph. As the results show, the proposed algorithm has given an increase in the PSNR value.

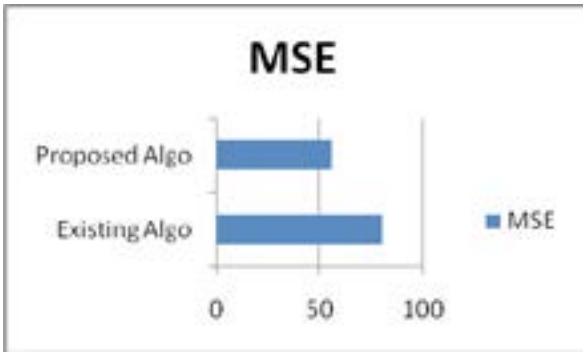

Figure 7. MSE comparisons.

As shown in Figure 7, the different parameters of new image are compared with the already existing image is made. The parameters define the images. The existing algorithm gives certain outputs which are made to compare with the new proposed algorithm. The outputs are shown in a bar graph. As the results show, in the proposed algorithm there is decrease in the MSE value.

5. Conclusion

The technique of image forgery is applied to mark the pixels from the image which are not similar to other image pixels. The panchromatic images are taken as input for the forgery detection. In the existing technique PCA algorithm is applied which will learn from the previous experience and drive new values based on training and trained datasets. The PCA algorithm will classify the images pixels according to their properties. In this work, improvement in been proposed in PCA algorithm for forgery detection. The proposed improvement is based on SIFT algorithm in the SIFT algorithm each pixel is analyzed according to pixel properties. The output of SIFT algorithm is given as input to PCA algorithm for classification. The simulation is performed in MATLAB and it is been analyzed that accuracy is improved, fault detection rate is reduced. In future further improvement can be applied in proposed algorithm by implement nearest neighbor classifier for image classification.

6. References

1. Murali S, Govindraj B, Chittapur C, Prabhakara HS, Basavaraj S, Anami A. Comparison and analysis of photo image forgery detection techniques. IJCSA. 2012; 2(6):1–1.
2. Gomase MPG, Wankhade MNR. Advanced digital image forgery detection- A review. IOSR-JCE. 2014; 4(3):80–3.
3. Rohini A, Maind M, Khade A, Chitre DK. Image copy move forgery detection using block representing method. IJSCE. 2014; 4(2):180–9.
4. Suresh G, Rao CS. RST invariant image forgery detection. Indian Journal of Science and Technology. 2016 Jun; 9(21):1–8.
5. Elwin JGR, Kousalya G. Image forgery detection using multidimensional spectral hashing based polar cosine transform. Indian Journal of Science and Technology. 2015 May; 8(S9):1–12.
6. Kalaivani R, Sudhagar K, Lakshmi P. Neural network based vibration control for vehicle active suspension system. Indian Journal of Science and Technology. 2016 Jan; 9(1):1–8.
7. Anitha K, Leveenbose P. Edge detection based salient region detection for accurate image forgery detection. IEEE. 2014; 12(10):1–4.
8. Moreno R, Puig D, Julia C, Garcia MA. A new methodology for evaluation of edge detectors. Proceedings of the16th IEEE International Conference on Image Processing (ICIP); Cairo. 2009. p. 2157–60.
9. Swaminathan A, Wu M, Liu KJR. Digital image forensics via intrinsic fingerprints. IEEE Transactions on Information Forensics and Security. 2008; 3(1):101–17.
10. Mikolajczyk K, Schmid C. A performance evaluation of local descriptors, pattern analysis and machine intelligence. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2005; 27(10):1615–30.
11. Gupta G. Improved median filter and comparison of mean, median and improved median filter. IJSCE. 2011; 1(5):819–27.
12. Maeno K, Nagahara H, Shimada A, Taniguchi RI. Light field distortion feature for transparent object recognition. IEEE explore Computer Vision Foundation. 2013; 6(1):2786–93.