Image Forgery Detection for Digital Image Resolution Using K-Component Analysis and PSO Algorithm

Sonia Dosanjh[1], Ms Ramanjot Kaur [2]
[1]M.*Tech (Scholar),* [2]*Assistant Professor*
Department of Computer Science Engineering and Information Technology
DIET, Kharar, SAS Nagar Punjab.

Abstract - In today's digital age, digital images form an important part of communication. Several tools and software's are available that can manipulate any given image. Therefore, verifying the authenticity of digital images becomes paramount in today's context. There is an increasing demand to identify the duplicate or forged images from original digital images that are not modified. There are two kinds of digital image forgery detection, copy-move and image splice and several other techniques like blurring, interference, scaling etc. Copy and Move forgery Image technique is a malicious tampering method with DIP (Digital Image Processing), where a part of image is copied and pasted within the image to conceal the significant details of an image without any noticeable signs of manipulation. The proposed method is developed with both the block that depends on the feature extraction and clustering based methods to extract the forged features more precisely. The proposed method mainly helps in matching similar features extracted from each wavelet blocks (LL, LH, HL and HH) by evaluating the product between the vector and values. PSOA algorithm is used to extract the filtered and optimized extracted features to match the edges. The experimental algorithm of the proposed method on implementation indicates that it can extract more accurate values at 98.5 % and with more precise results as compared with previous forgery detection techniques.

Keywords - *Forgery Image, DIP, Feature Extraction, SIFT, Wavelet and PSOA.*

I. INTRODUCTION

With the current development in technology, image manipulation and particularly image splicing has been termed as a regular and established concern. The swift growth in commercial image editing programs and software for instance, Adobe Photoshop has significantly elevated the number of forged, doctored and tampered images on daily basis [1]. A digital picture is in the form of the bits and can categorise in form of the bit deepness. A binary image is in the form of 0 and 1in single bit whereas black and white image is in multiple bit form [1]. Digital Image Forgery is the method that is related to digital picture. The method of the establishment of the fraud picture is done through graphical form, edition of the software system, Corel draw method, Adobe Photoshop technique [2].

Image forgery detection is needed to prevent alteration of images and restore some trust in digital images. It is applied in areas such as journalism, digital forensic science and surveillance systems. The availability of powerful image processing and editing software makes it easy to create, alter and manipulate digital images. With that, the issue of verifying the authenticity and integrity of digital images is becoming increasingly important. There are two categories of image forgery detection techniques: active and passive. Active, also known as intrusive detection techniques require a form of digital signature to be embedded in the image at the instance of its creation. However, not all digital devices are able to implant such signatures when capturing images. On the other hand, passive also referred to as non-intrusive or blind approaches examine the image blindly without reliance on any embedded information. Although a passive approach has wider scope of usefulness, it is a computationally expensive process [3].

Copy-move forgery is one of the tampering methods used to manipulate digital images. It is done by duplicating a region of the original image and pasting it onto another region of the same image. Various methods have been proposed to passively detect copy move image forgery [4-5].

In proposed algorithm used the main idea is to describe k centres, one for both clusters. These centres should be positioned in a cunning way because of different location causes different result [6,7]. So, the better choice is to place them as much as possible far away from each other. The following step is to take each point going to an assumed data set and associate it to the nearest centre. When no point is pending, the first step is completed and an early group age is done. At this point we need to re-calculate k new centroids as bray centre of the clusters resulting from the previous step. After we have these k new centroids, a new binding has to be done between the same data set points and the nearest new centre [15]. A loop has been generated [8-9].

Discrete wavelet transform is utilized in image compression. The compression in general way is an approach that applied in digital image processing. The main work is to minimize the size of an image to fit in a dataset. Along with this, it is preferred as a successful technology in image processing [10].

Technique for reduction of simulation of non-linear functions and discovered through simulation of a simplified social model, thus the social meta-phor is described, though the method stands without symbolic support. PSO described that the optimization concept in terms of its precursors, explained surveying the phases of its development from social simulation to reducer [11].

II. LITERATURE SURVEY

Al-Hammadi, M. M and Emmanuel, S et al., 2016 [16] focused on detection of image forgery utilising speedup robust feature approach on the basis of the copy movement forgery detection technique. This method enhances the detection of key factor through pre-processing of the picture through unique image. The evaluated result proposed a technique of actual speedup robust feature utilising database with smaller forgery.

Ramu, G., et al., (2017) [17] briefly described the concept of image forgery detection specifically for the high resolution pictures. The proposed approaches was SIFT and RANSAC technique. Cloning was a harmful tampering form of attack in which the region of image is copied and paste somewhere else to secrete the crucial details without manipulation. Therefore, the question related to authentication was raised. The new primitive approach was composed of block based technique and feature extraction technique particularly to find out the regions accurately. Tentacle matching was a technique to match similar features from each block through dot product. Subsequently, RANSAC (Random sample consensus) approach was attained which was capable of capturing the results accurately rather than existing techniques for fraud detection.

Gunjan Bhartiya et al., 2016 [18] defined, a technique to detect forgery in JPEG image was accessible and an algorithm was developed to classify the image blocks as forged or non-forged grounded on this classification. The method created better consequences than the prior methods which use the prospect based method for detecting forgery.

Mohd Dilshad Ansari, et al., 2014 [19] described with the improvement of the digital image dispensation software and deletion tools, a digital image could be definitely manipulated. The detection of image operation was very important since an image could be used as legal evidence, in forensics surveys, and in many other arenas. The pixel-based image forgery detection aims to verify the reality of digital images without any previous knowledge of the original image. There were numerous ways for tampering an image such as splicing or copy-move, re-sampling an image, adding and removal of any entity from the image.

Tu Huynh-Kha et al., 2016 [20] defined method to detect forgery by copy-move, splicing or both in the same image. Multi-scale, which limits the computational complexity, was used to check if there was any forged in the image. By relating one-level Discrete Wavelet Transform, the sharped edges, which were traces of cut-paste manipulation, were high frequencies and detected from LH, HL and HH sub-bands. A threshold was projected to filter the apprehensive edges and the morphological operation was applied to reconstruct the boundaries of forged regions. If there was no shape fashioned by dilation or no highpoint sharped edges, the image was not faked. In case of forgery image, if a region at the other position was similar to the defined region in the image, a copy-move was established. If not, a splicing was detected. The apprehensive region was extracted the feature using Run Difference Method and a feature vector was created. Searching regions had the same feature vector which was called detection phase.

III. RESEARCH METHODOLOGY

To design a framework to detect the forged data in the splice image using feature extraction method to fetch the unique properties in the form of texture form like as a eigen values and eigen vector. 2D transformation method used to filtered the image and divide the splice image into 8*8 bit size blocks. Clustering method is used to divide the splice image in the form of two clusters like as a CLUSTER 1 and CLUSTER 2. After that data division is used to implement an optimization method to reduce the feature size into two operators used.

i). Updating x –position (Public Best)

ii). Updating y-position (Global Best)

Proposed feature selection using PSOA algorithm based on feature selection to detect the forgery image. To compute the proposed performance metrics like as a FAR, FRR, Accuracy and MSE and compared with the existing work.

Proposed flow chart is explained step wise:

1. The image from data base is uploaded. Converting black and white image size for the reduction of the pixels of picture matrix and plotting the histogram to determine the numerical information in amount of the bits.

2. Conversion of RGB picture in the colour area.

3. Relate the distributed picture size RGB image to black and white image. Then distribute the picture in three level phases in level-0, level -1, level-2. Using K means clustering for conversion of format to form clusters. The description of DWT approach for transformation of clustered information and extraction of information utilising LL, HL, LH, HH.

4. Demonstrate the extraction of feature using PCA. That is defined experimentally for recognising the smoothness of feature likes as Eigen value and Eigen vector.

5. Implementation of planned approach method where Particle Swarm Optimisation is utilised for the classification of the forged area on the basis of the specific characteristics.

6. Calculate Specificity, Sensitivity, FPR, FNR and Accuracy for every decayed blocks and analyse the experimental metrics on the basis of the previous research.

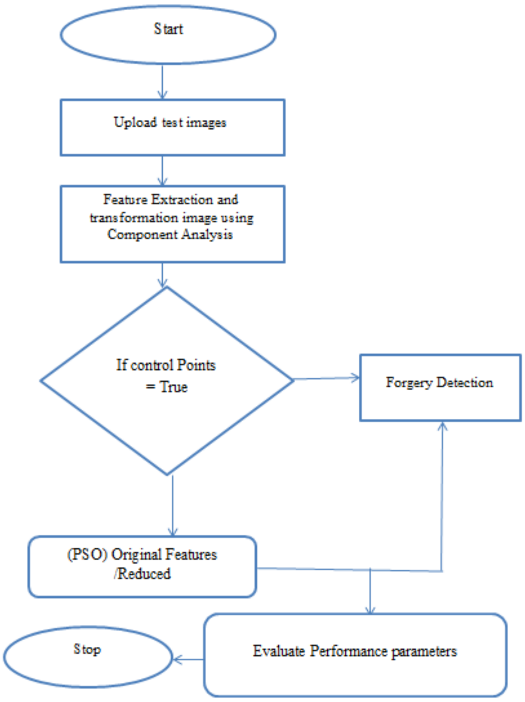
Start
Upload test images
Feature Extraction and transformation image using Component Analysis
If control Points = True
Forgery Detection
(PSO) Original Features /Reduced
Evaluate Performance parameters
Stop

Figure 1: Research Flo Chart

IV. RESULT AND DISCUSSIONS

A. Dataset - CASIA v1.0 is a data set used in image forgery that is focused on the joining recognition approach. The joining of the picture is determined as the easy cut and paste method of picture areas from one picture on similar image in absence of pre-processing. The essential method of the altering [11] CASIA v1.0 data base consists 800 authenticated and 921 joined colour pictures of dimension 384×256 pixels with JPEG arrangement [12]. The genuine picture is mainly collected from the Corel picture database and also acquired from the digital cameras. In next procedure, confidential pictures are discriminated in to various groups like as animal, physical, construction, atmosphere, herbal, object, environment in accordance to component and consideration of pre-processing of joined pictures [13].

Figure 2: Copy move Forgery Database [14]

B. Results - The planned image processing technique is used with graphical user interface in MATLAB 2016a. Defined that the proposed work steps are (i) Image Acquisition (ii) Data pre-processing (iii) Cluster method (iv) Feature Extraction and (v) Optimization Process.

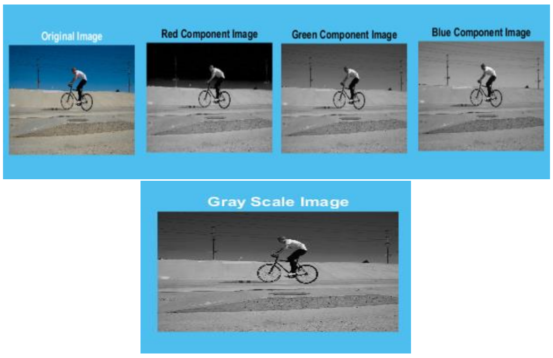

Figure 3: Uploaded Picture and Analysis of Component

The given figure shows the uploading of the actual image from the data base. Then conversion of RGB to black and white image is done. Above figure describe the RGB analysis of the component. Computed RGB values are used in an approach to determine the colours that are required to utilise on system display.

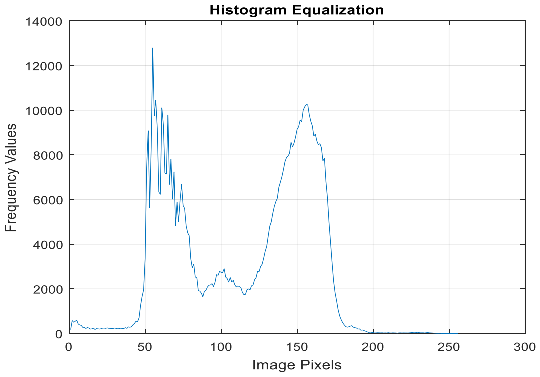

Figure 4: Picture Histogram

Here plotting of the histogram that works as the graph demonstration of the average distributed in digital picture. After that, amount of pixels for tonal assessment. The whole picture is segmented at time are selected for the unique picture for the histogram.

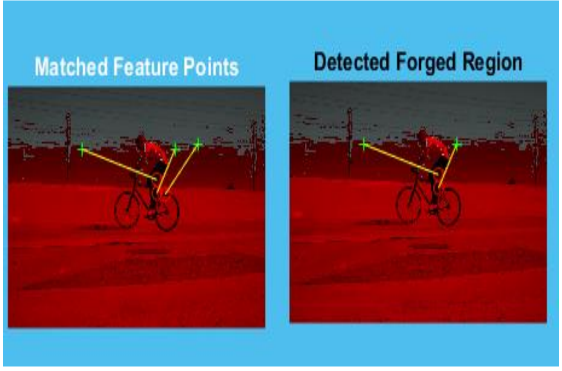

Figure 5: Matching of Data and Forgery surface Detection in the Image

Above figure defined that the matched feature-points and Detected Forgery area in image. Detection is done by testing phase and when the features are similar in training and testing phase. Then, calculate the performance parameters such as Specificity Rate, Sensitivity Rate and Accuracy Rate.

Table 1:- Proposed Performance Parameters

Metrics	Values
Accuracy rate (%)	98.9
False Positive Rate	0.032
False Negative Rate	0.64
Sensitivity	0.993
Specificity	0.9964

Table 2: Comparison between Proposed And Existing Work

Metrics	Proposed Work	Existing Work
Accuracy Rate (%)	98.9	97.6
Sensitivity Rate	0.993	0.96
Specificity Rate	0.9964	0.90
False Positive rate (%)	0.32	0.80
False Negative rate (%)	0.64	0.40

Given table describe the planned parameters and comparison analysis such as accuracy rate, specificity, sensitivity, FPR and FNR.

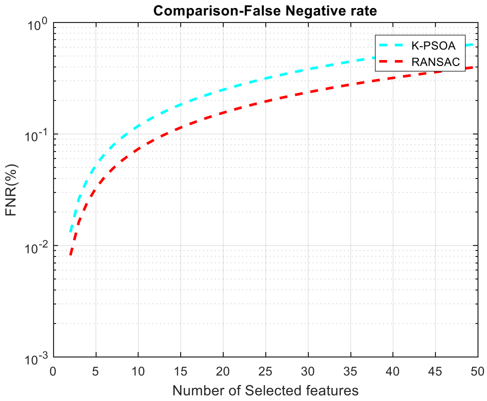

Figure 6: Comparison – False Negative Rate (%)

Above figure shows about the comparison between proposed and existing methods. FNR is improved with proposed method. It is a test consequence that indicates that a situation doesn't hold. Other words, erroneously, no-effect has be inferred. If a single situation is verified for and the result of test is in accurately that the situation is absent.

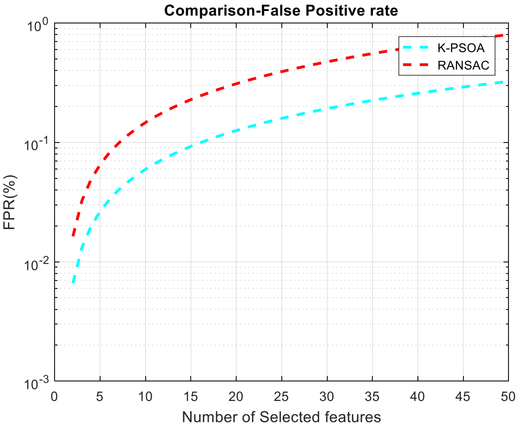

Figure 7: Comparison - False Positive Rate

The given figure describe the comparison among planned and previous research work metrices in FPR actual class is absent and predicted value is present. It is proportional of positives which produce negative test results with the test that is the situation probability of a negative test result defined that the situation being looked for is present.

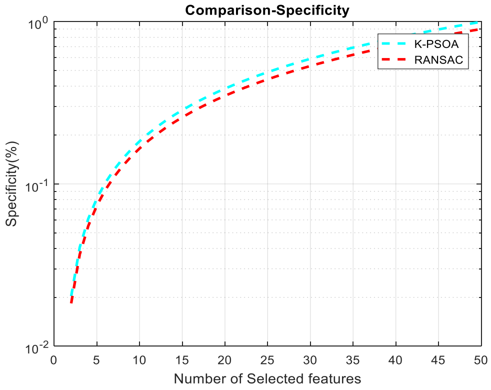

Figure 8: Comparison – Specificity

Specificity demonstrate the parametric analysis to improve the PR in copy-movement forged picture.

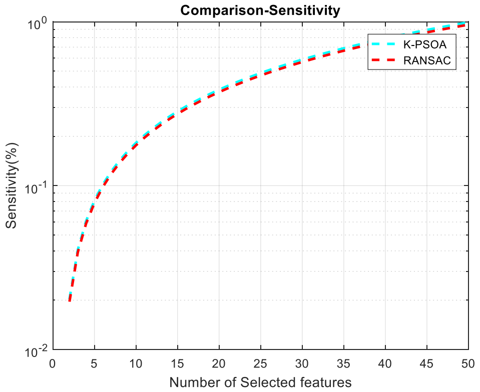

Figure 9: Comparison – Sensitivity

Fig 9 Comparison defined that the comparison between proposed and existing works. Specificity means true positive rate and proposed method used to improve the sensitivity rate.

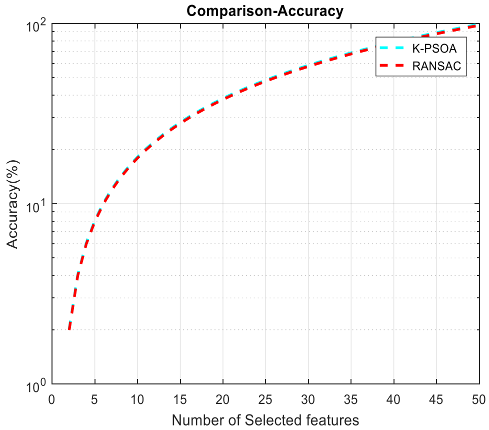

Figure 10: Comparison – Accuracy Rate

The given figure describes the comparison analysis among planned and previous research work. In planned approach accuracy rate value is 98.9% and 97% to enhance the accuracy rate and reduction of error rate.

V. CONCLUSION AND FUTURE SCOPE

Forged pictures are utilised as important technique for the detection of the forged images. Various applications areas of the forged images are extra advertisement, hide the occasion, misinterpretation. Forged images are used as the proof of the inquiry in forensic technology. Various pictures are placed together for the inquiry purpose, that pictures may be suspicion as forged or not. Digital images are used for different aspects so the authentication is crucial to determine the identity and confidentiality of the digital pictures. However, utilisation of digital pictures has become common, so there is developed for digital pictures with help of the existing methods. The editing software techniques create forgeries in digital pictures in absence of the proof that can be recognised by human eye. In proposed research, feature of images are extracted accurately through feature extraction and clustering based technique. Proposed technique helps in the addition of the matched characteristics from each wavelet blocks (LL, LH, HL and HH). It then computes the product between the vector and values. The filtration and the optimisation of the extracted features of matched edges are done using PSOA algorithm. Experimental analysis has done through performance metrics like as accuracy up to 98.7% by comparing with exiting method.

In future scope, various techniques can be drawn out for detection of forgery through post processed method that can be implemented using CNN methods and Deep Learning method.

VI. REFERENCES

[1]. Jadhav, M. R., Chavan, M. S., Patil, M. K., Shivankar, M. S., and More, M. M.(2015) Survey On Fraud Image Detection, International Journal of Innovative Research and Creative Technology,vol 1(6), pp. 523-526.

[2]. Garg, T., and Saini, H. (2017). A Review on Various Techniques of Image Forgery Detection, International Journal of Engineering Technology Science and Research, *vol, 4(4)*,pp. 490-493.

[3]. Elwin, J. G. R., Aditya, T. S., and Shankar, S. M. (2010). Survey on passive methods of image tampering detection. In *2010 International Conference on Communication and Computational Intelligence (INCOCCI), vol2 (3),* pp. 431-436, IEEE.

[4]. Ansari, M. D., Ghrera, S. P., and Tyagi, V. (2014). Pixel-based image forgery detection: A review. *IETE journal of education*, vol *55*(1), pp. 40-46.

[5]. Bayram, S., Sencar, H. T., & Memon, N. (2008). A survey of copy-move forgery detection techniques. In *IEEE Western New York Image Processing Workshop* , vol 4(5), (pp. 538-542). IEEE.

[6]. Asghar, K., Habib, Z., & Hussain, M. (2017). Copy-move and splicing image forgery detection and localization techniques: a review. *Australian Journal of Forensic Sciences*, vol *49*(3), pp- 281-307.

[7]. Poisel, R., & Tjoa, S. (2011). Forensics investigations of multimedia data: A review of the state-of-the-art. In *2011 Sixth International Conference on IT Security Incident Management and IT Forensics, vol 3(2),* (pp. 48-61). IEEE.

[8]. Mishra, M., and Adhikary, F. (2013). Digital image tamper detection techniques-a comprehensive study. International Journal of Computer Science and Business Informatics, vol 2(3), pp:1306.6737.

[9]. Zhang, Z., Ren, Y., Ping, X. J., He, Z. Y., and Zhang, S. Z. (2000). A survey on passive-blind image forgery by doctor method detection. In *2008 international conference on machine learning and cybernetics*, Vol. 6(2), pp. 3463-3467.

[10]. Qureshi, M. A., and Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication*, vol *39(2)*, 46-74.

[11]. Garg, T., and Saini, H. (2017). A Review on Various Techniques of Image Forgery Detection. *vol*, *4(2)*,pp- 490-493.

[12]. Gill, N. K., Garg, R., and Doegar, E. A. (2017). A review paper on digital image forgery detection techniques. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* , vol 2(3), (pp. 1-7). IEEE.

[13]. Bharti, C. N., and Tandel, P. (2016). A survey of image forgery detection techniques. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* , vol 7(2), (pp. 877-881). IEEE.

[14]. Khanduja, D. K., and Gokhale, M. Y. (2010). Time domain signal analysis using modified haar and modified daubechies wavelet transform. *Signal Processing-An International Journal (SPIJ)*, vol *4*(3), pp. 161.

[15]. Boeringer, D. W., and Werner, D. H. (2004). Particle swarm optimization versus genetic algorithms for phased array synthesis. IEEE Transactions on antennas and propagation, vol 52(3), pp. 771-779.

[16]. Al-Hammadi, M. M., and Emmanuel, S. (2016). Improving SURF based copy-move forgery detection using super resolution. In *2016 IEEE International Symposium on Multimedia (ISM)vol 2(3),* (pp. 341-344). IEEE.

[17]. Ramu, Gonapalli, and SBG Thilak Babu. (2017), Image forgery detection for high resolution images using SIFT and RANSAC algorithm." In *Communication and Electronics Systems (ICCES), 2017 2nd International Conference on*, vol 2(2), pp. 850-854.

[18]. Bhartiya, Gunjan, and Anand Singh Jalal. (2014), Image forgery detection using feature based clustering in JPEG images." In Industrial and Information Systems (ICIIS), 2014 9th International Conference on, vol 3(2), pp. 1-5. IEEE.

[19]. Ansari, Mohd Dilshad, Satya Prakash Ghrera, and Vipin Tyagi.(2010), Pixel-based image forgery detection: A review." IETE journal of education 55, no. 1 , pp-. 40-46.

[20]. Huynh-Kha, Tu, Thuong Le-Tien, Synh Ha-Viet-Uyen, Khoa Huynh-Van, and Marie Luong. (2016), A Robust Algorithm of Forgery Detection in Copy-Move and Spliced Images." International Journal of Advanced Computer Science & Applications vol 1(7) pp. 1-8.