Image Forgery Detection for Image Resolution Using K-PCA and Genetic Algorithm

Shuchita Aggarwal[1], Er. Deepinder Kaur[2]
[1]M.Tech student, [2]Assistant professor
[12]SUSCET Tangori, Mohali,India

Abstract- The growth in commercial image modification software and program for instance like as an Adobe Photoshop has importantly elevated the number of tampered digital images on a daily basis. This situation has outcome into extreme results, reducing the authentication and reliability of such images. Authentication of the image suffers from serving threats due to the rise of powerful Digital Image editing tools that easily change the image content without leaving any visible traces of such modification. The splicing can be done by forging one or more edge from the source image and pasted into a target image to produce a composite image is called as spliced image. Copy and Move forgery Image is malicious tampering hijacked with Digital Image Processing, were a part of the image is copied and pasted within the image to conceal the significant details to image without any notice suggestions of manipulation. This kind of tampering hijackers leaves a huge question of authenticity of images,several methods are implemented in the previous few years to detect the forgery after powerful software's are developed to change the image. Forgery detection in existing work is done on .jpg images. Feature Extraction methods used in copy-move image forgery detection requires a high interval of time. The major problem found in existing papers as follows:-
(i) High Computation Time
(ii) Distortion
(iii) Less accuracy rate
(iv) False errors.
Need to reduce the above problems in forgery detection by using K-PCA and genetic algorithm. In this work, we have designed and implemented a K-PCA with Wavelet transformation method to detect the copy-move forgery image in images. Genetic algorithm to optimize the error rates and match the features. Enhanced the performance metrics computed as a False Positive Rate, Accuracy rate and False Positive rates, Sensitivity, Specificity.

Keywords- K-PCA (K-Principle Component Analysis), GA (Genetic Algorithm), Block –Wise and Copy- move forgery image.

I. INTRODUCTION

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. Act, also known as intrusive, detection techniques requires 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[1]. 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 a wider scope of usefulness, it is a computationally expensive process. Image forgery detection is needed to prevent alteration of images and restore some trust in digital images[4]. 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. Act, also known as intrusive, detection techniques requires 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 a wider scope of usefulness, it is a computationally expensive process [2].

Several applications such as splicing image detection investigations of digital images for law enforcement agencies, image surveillance, and presenting video evidence in courts of law need more advanced detection and authentication techniques to prove the trustworthiness of digital images. The present research provides image authentication techniques that play a key role in detecting and identifying image splicing forgery [3].

II. REVIEW OF LITERATURE

Ramu, G., et al., (2017) [17] briefly described the concept of image forgery detection specifically for the high resolution pictures. The proposed approaches where SIFT and RANSAC technique. Cloning was a harmful tampering form of attack in which the region of the image is copied and paste somewhere else to secrete the crucial details without manipulation. Therefore, the question related to authentication 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 to capture the results accurately rather than existing techniques for fraud detection. **Bhartiya, G., 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. **Ansari, M.D., 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. **Huynh-Kha, T., 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 sharper edges, which were traces of cut-paste manipulation, 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 high-point sharper 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 phases.

III. PROPOSED ALGORITHM

K-means is one of the greenest unsupervised learning algorithms that solve the well-known clustering problem. The procedure follows a simple and easy way to categorize a given data set through a convinced number of clusters (assume k clusters) fixed a priority. The main idea is to describe k centers, one for both clusters. These centers should be positioned in a cunning way because of different location causes different result. So, the better choice is to place them as much as possible far away from each other.[5,6]

Advantages of K-mean Clustering

- Fast
- Robust and Easier to understand.[7,8]

Component Analysis using the PCA algorithm

In feature extraction technique is used to recover most revealing terms from amount of matrix. This study used Component Analysis technique to calculate and study the Eigenvector and values to find the feature values and then to direct individual data with its principle components / Eigen Vectors.[9]

DWT (Discrete Wavelet Transform) Method

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]. The first finder of wavelet transform is Grossmann and Morlet. DWT is a mathematical approach which associated to functions and to describe the data. AS usual it is considered as a signal process with extreme efficiency. The average value is zero and wavelet initiated at up and downs of axis [11]. DWT is most preferable approach for both signal processing and image compression. The process begins when a signal is divided into a group of functions and it is called as wavelet. The wavelets are derived from a basic mother wavelet with the use of both dilation and shifting procedure. The storage of images in wavelet is more rather than storage in pixel blocks. The edges are rough which useful to eliminate blocks in images or patterns [12].

Types of DWT (Discrete Wavelet Transform)

In discrete wavelet transform, two basic functions are used to transfer the data. First one is Haar transform and another is Daubechies Transform.

- **Haar Transform:** It is the basic and simplest transformation used in DWT. This wavelet worked on discontinuity and based on step functions. Haar is introduced by Hungarian mathematician namely Alfred Haar. It simply collaborate the input data, afterwards stores the difference and sent the sum for further procedure. Haar transform repeats its process again and again to obtain the final sum of input data [13].
- **Daubechies Transform:** Daubechies is the most unique and high demand wavelet transform. Other name is orthogonal wavelet. It is the fundamental requirement that completes the discrete wavelet transform. The transform is derived from dbN as its name implies the N for name and db for sur-name Classes of DWT linked to the Daubechies filters due to co-relation with the orthogonal wavelets [13] [14].

Genetic Algorithm

Genetic algorithms are the computerised algorithms that attained attention due to the simple and executable process to find out the best solution of a number of solutions. The procedure is dependent upon the natural selection of individuals form the given population.

- Selection: Selection operator sometimes called as reproduction operator which is the first operator to initialize the process of genetic algorithm.
- Crossover: this is the second most crucial operator that is performed after the selection process. The two individuals are selected from the overall population.

- Mutation: This is the last operator which takes place to modify and alter the any requirement which is necessity to complete the process of genetic algorithm in the end. [15,16].

IV. METHODOLOGY

Image forgery is the common and easy techniques are image splicing. Image splicing is act of cropping regions of an image and pasting it into the same or different image to create a novel forged image. So deciding about the authenticity of an image has become increasingly difficult.

In this research work, we try to reduce the problem in image slicing dataset. The simple way to detect the forgery image and compute the performance parameters like as a FAR, FRR, Accuracy and Means Square Error Rate and Compared with the existing work.

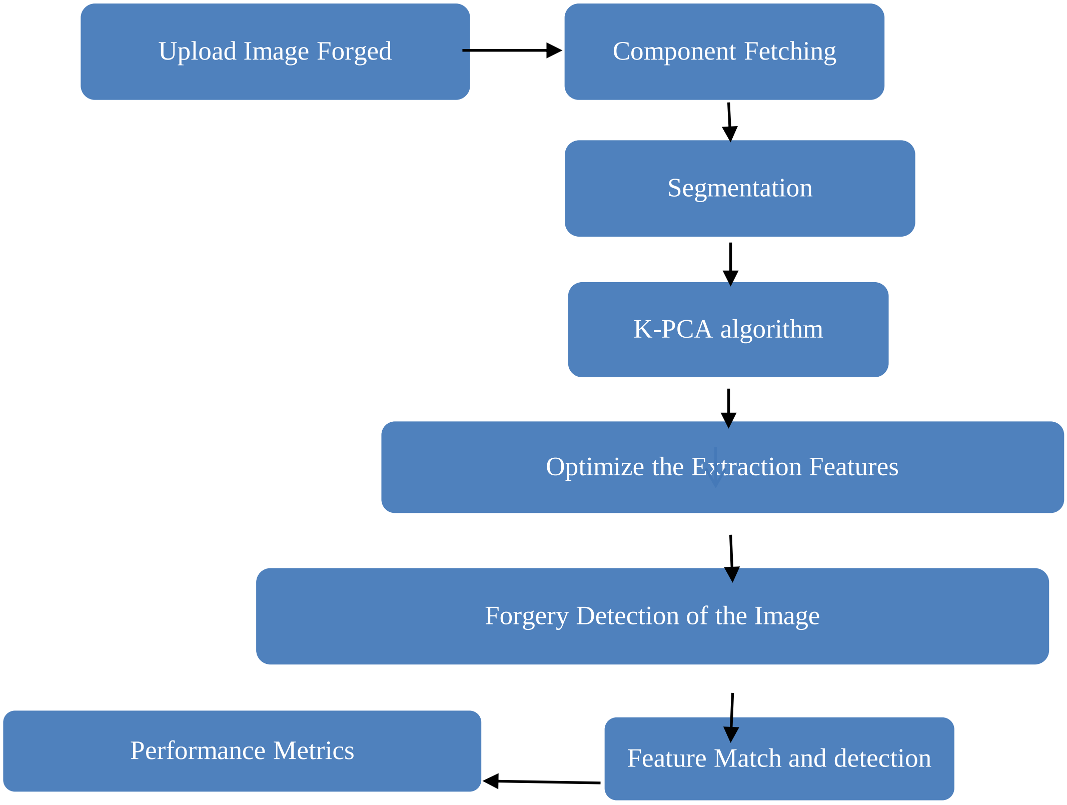
Upload Image Forged
Component Fetching
Segmentation
K-PCA algorithm
Optimize the Extraction Features
Forgery Detection of the Image
Feature Match and detection
Performance Metrics

Fig.2: Block diagram of the proposed method

The design a framework to detect the forgery, data in the splice image using feature extraction methods to fetch the unique properties in the form of texture form like as a eigen values and eigen vector. DWT used to filter the image and divide the splice image into 8*8 bit size blocks. Clustering method used to divide the splice image in the form of two clusters like as a CLUSTER 1 and CLUSTER 2. After that data division implement an optimization method to feature reduce the size into three operator used i.e, (i) Selection (ii) Crossover and (iii) Mutation detect the forgery image. To compute the performance metrics like as a FAR, FRR, Accuracy and MSE and compared with the existing work.

V. RESULTS AND DISCUSSION

This section determines the evaluated results of the proposed digital image processing concept for forgery detect in image splicing JPG images. Also the percentage of forgery detect the images determined with the overall accuracy of the concept is evaluated.The proposed image processing concept is implemented in MATLAB with GUI (Graphical User Interface). The considered GUI is shown in figure 4.2.1. Here, the considered buttons are Image Acquisition, pre-processing, clustering, feature extraction and optimization as well as classification.

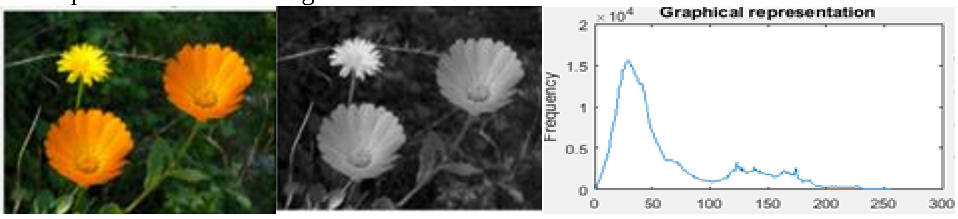

Fig.3: Uplaod Image , Gray scale and Histogram Image

The process of image forgery detection is called image acquisition. Detect the rgb2gray conversion and segmentation using clustering algorithm used to detect the level 0,1 and 2 segmented image. Implement the feature extraction approach to find the unique properties in the form of eigen values and eigen vectors. Extracted features we apply the optimal approach to classify and detect the forgery area in the image.uploads the original image from the data set. Convert the rgb2gray scale form image. We plot the histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

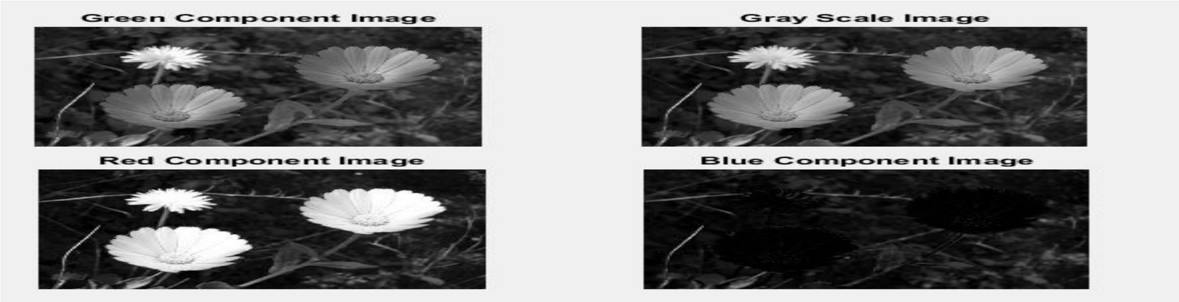

Fig.4: Component Fetching

The above figure defined that the rgb component calculates. RGB (red, green, and blue) refers to a system for representing the colors to be used on a computer display. Red, green, and blue can be combined in various proportions to obtain any color in the visible spectrum.

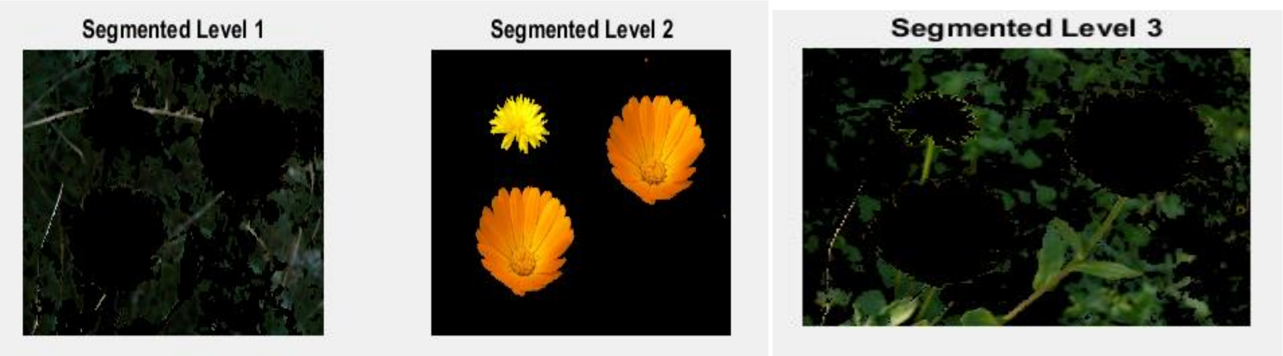

Fig.5: Segmentation

The above figure represents that the segmentation applied to identify the region area. We apply the k-mean clustering approach to calculate the data in cluster form and segmentation level defined images LEVEL-1, LEVEL-2 and LEVEL-0.

Fig.6: Block Wise Method (DWT)

The above figure shows that the DWT is most preferable approach for both signal processing and image compression. The process begins when a signal is divided into a group of functions and it is called as wavelet. The wavelets are derived from a basic mother wavelet with the use of both dilation and shifting procedure. The storage of images in wavelet is more rather than storage in pixel blocks. The edges are rough which useful to eliminate blocks in images or patterns.

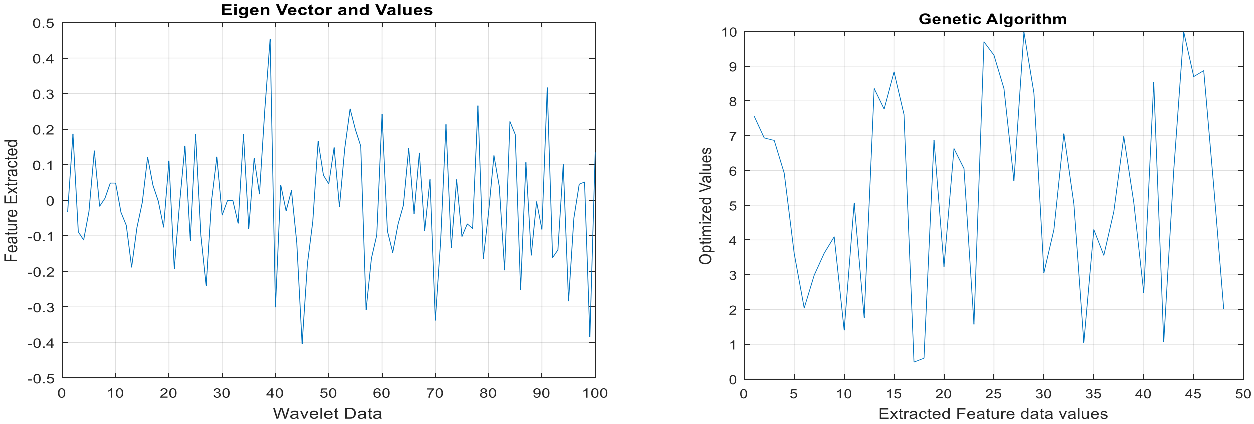

Fig.7: Feature Extraction and Genetic Algorithm

The above figure defined that the feature extracted using principle component analysis. We calculate the features in the form of Eigen Values and Eigen Vectors. Extracted Features save in database. The above figure shows the reduce the extracted features in the form of graph representation. In genetic optimization algorithm used to optimize the features only selected the relevant features.

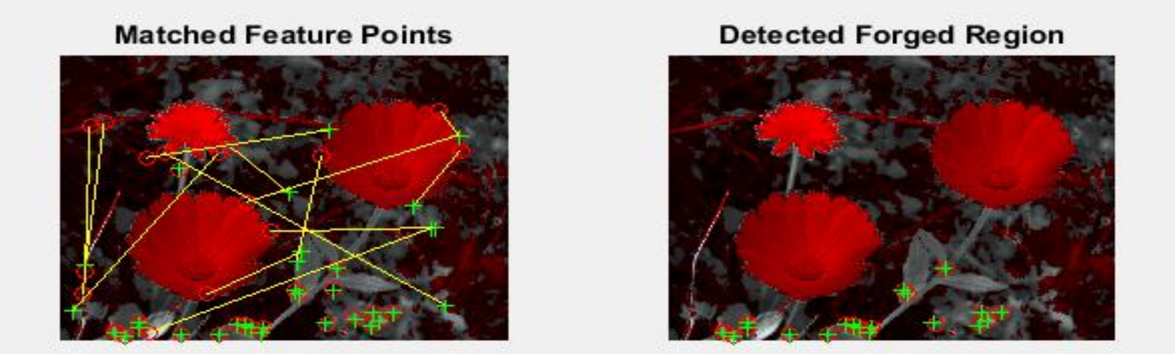

Fig.8 Matched Data and Forgery Area Detect in the Image

The above figure defined that the testing phases to identify features and matching process. In testing Phase, match the features in training and testing phases. If features are matched in both cases then detect the forgery area. And calculate the performance parameters i.e specificity rate, accuracy and sensitivity.

TABLE 1:- PROPOSED PARAMETERS

Metrics	Values
Accuracy rate (%)	98%
False Positive Rate	0.012
False Negative Rate	10.0
Sensitivity	99%
Specificity	96.6%

TABLE 2:- COMPARISON BETWEEN PROPSOED AND EXISTING WORK

Metrics	Proposed Work	Existing Work
Accuracy Rate (%)	99%	98%
Sensitivity Rate	96.6%	96%
Specificity Rate	99.6%	98%
False Positive rate (%)	0.012	0.08
False Negative rate (%)	0.01	0.04

Table 1 and 2 defined that the proposed parameters and comparison parameters like as a accuracy rate, specificity, sensitivity, false positive rate and False negative rate.

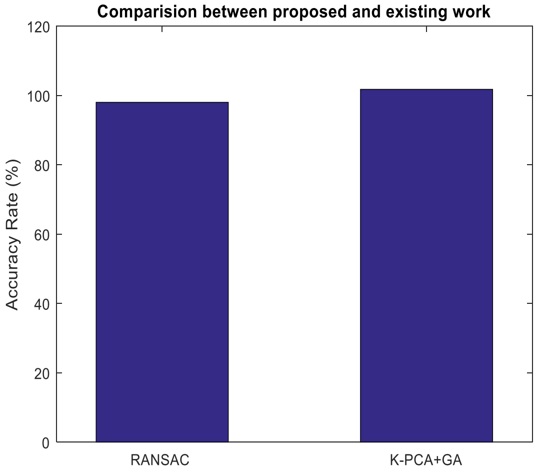

Fig.9: Comparison – Accuracy (%)

The above figure shows that the comparison between the proposed and existing work using Accurate rate value is 98% and 97%. In the proposed method to improve the accuracy rate and reduce the error rates.

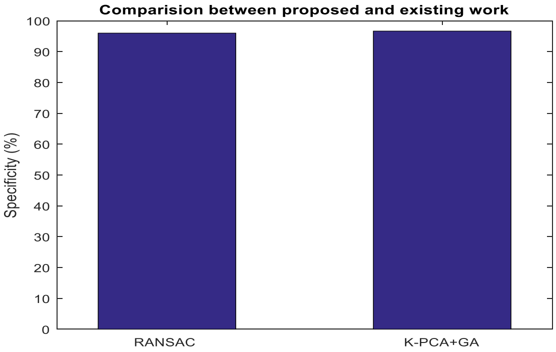

Fig.10: Specificity – Comparison

The specificity performance parameters enhance the positive rate in the copy-move forged image.

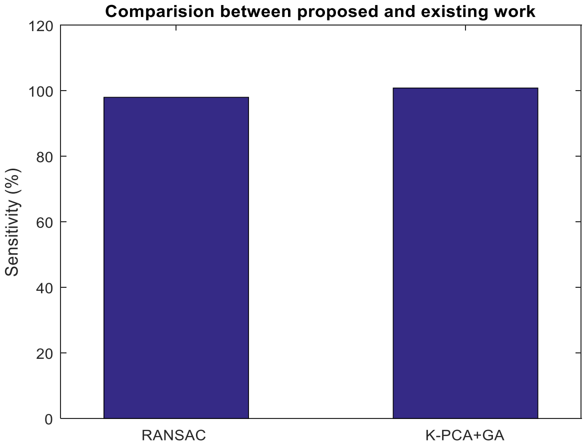

Fig.11: Sensitivity – Comparison

The sensitivity comparison defines that the prediction of the positive parameters and improve the proposed parameters.

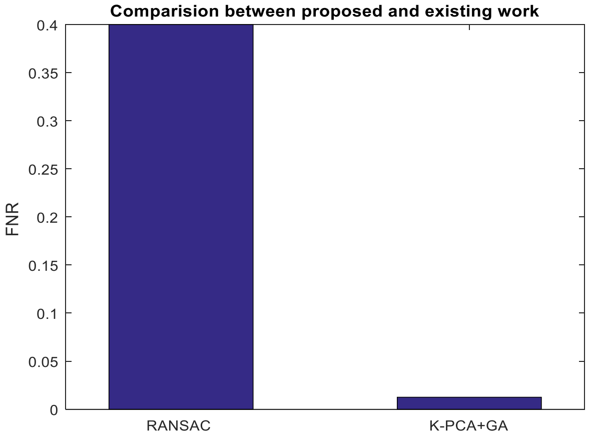

Fig.12: False Negative Rate – Comparison

The above figure defines that the comparison between false negative rate parameters. If real class is yes, but predicted class in no.

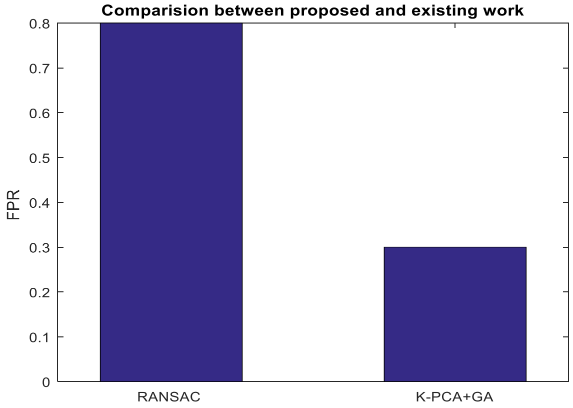

Fig.13: False Positive Rate – Comparison

The above figure defines that the comparison between the proposed and existing work parameter in false positive rate rate real class is no and prediction class is yes format.

IV. CONCLUSION AND FUTURE SCOPE

Digital Image processing is a powerful availability programs like as a photo Shop, makes it relatively simple to design a digital forgery from one or various images. Due to the development of IP and CT software, DIF (Digital Image Forgery) has been increasingly simple to perform. However, DIs are a famous source information, and the reliability of DIPs is thus becoming a significant issue. In current years, more and more researchers have activated two main focus on the problem of DI tampering. In existing work, kinds of image tampering a common manipulation of DIs are cut-paste and copy-move forgery, which is to paste one or various copied edge of an image onto another section of the same image or another image. In abstract cut –paste forgery image, forgers normally Improve the image contrast. Several papers are studying have been analyzed , numerous forgery detection methods are studied. The implementation is new or novel as it uses K–PCA algorithm. It is more complex and costly as we adopted as we adopted both block-wise depend and feature –point algorithms. We further used K-PCA and GA algorithm to match and detect the features the tampered region. The overall accuracy rate is 99% with database copy-move and splicing database of 80 images.

In future work, we would like to design and implementation detection process with more recall rate and precise rate and also with some other tampering methods like as a splicing and copy-paste images.

In this research work, a new dataset is created for CMFD that adds more changed pictures that were performed deliberately by professionals. The obtained data set is an open source and free to reduce as benchmarking for more comparisons. According to this novel research, it is highly re-commended that reducing the multiple clustering methods or even using the FCM by Matric optimization rather than the sequential reduction done.

V. REFERENCES

[1]. Farid, H. (2009). Image forgery detection. IEEE Signal processing magazine, 26(2), 16-25.

[2]. Zhang, J., Feng, Z., & Su, Y. (2008, November). A new approach for detecting copy-move forgery in digital images. In Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on (pp. 362-366). IEEE.

[3]. Lin, H. J., Wang, C. W., & Kao, Y. T. (2009). Fast copy-move forgery detection. WSEAS Transactions on Signal Processing, 5(5), 188-197.

[4]. Luo, W., Huang, J., & Qiu, G. (2006, August). Robust detection of region-duplication forgery in digital image. In Proceedings of the 18th International Conference on Pattern Recognition-Volume 04 (pp. 746-749). IEEE Computer Society.

[5]. Shih, F. Y., & Yuan, Y. (2012). 16 A Comparison Study on Copy–Cover Image Forgery Detection. Multimedia Security: Watermarking, Steganography, and Forensics, 297.

[6]. Shivakumar, B. L., & Baboo, L. D. S. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology.

[7]. Van Lanh, T., Chong, K. S., Emmanuel, S., & Kankanhalli, M. S. (2007, July). A survey on digital camera image forensic methods. In 2007 IEEE international conference on multimedia and expo (pp. 16-19). IEEE.

[8]. Gharehchopogh, F. S., Jabbari, N., & Azar, Z. G. (2012). Eval7uation of fuzzy k-means and k-means clustering algorithms in intrusion detection systems. International Journal of Scientific & Technology Research, 1(11), 66-72.

[9]. Li, J., Li, X., Yang, B., & Sun, X. (2015). Segmentation-based image copy-move forgery detection scheme. IEEE Transactions on Information Forensics and Security, 10(3), 507-518.

[10]. Gupta, D., & Choubey, S. (2015). Discrete wavelet transform for image processing. International Journal of Emerging Technology and Advanced Engineering, 4(3), 598-602.

[11]. Chowdhury, M. M. H., & Khatun, A. (2012). Image compression using discrete wavelet transform. International Journal of Computer Science Issues (IJCSI), 9(4), 327.

[12]. Shensa, M. J. (1992). The discrete wavelet transform: wedding the trous and Mallat algorithms. IEEE Transactions on signal processing, 40(10), 2464-2482.

[13]. Mehra, I., & Nishchal, N. K. (2015). Optical asymmetric image encryption using gyrator wavelet transform. Optics Communications, 354, 344-352.

[14]. Khanduja, D. K., & Gokhale, M. Y. Time Domain Signal Analysis Using Modified Haar and Modified Daubechies Wavelet Transform. Signal Processing-An International Journal (SPIJ), 4(3), 161.

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

[16]. Iquebal, M. A. (2005). Genetic Algorithms and their Applications: An Overview (Doctoral dissertation, Ph. D. Agricultural Stat. Roll).

[17]. Ramu, G., & Babu, S. T. (2017, October). Image forgery detection for high resolution images using SIFT and RANSAC algorithm. In Communication and Electronics Systems (ICCES), 2017 2nd International Conference on (pp. 850-854). IEEE.

[18]. Bhartiya, G., & Jalal, A. S. (2014, December). Image forgery detection using feature based clustering in JPEG images. In Industrial and Information Systems (ICIIS), 2014 9th International Conference on (pp. 1-5). IEEE.

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

[20]. Huynh-Kha, T., Le-Tien, T., Ha-Viet-Uyen, S., Huynh-Van, K., & Luong, M. (2016). A Robust Algorithm of Forgery Detection in Copy-Move and Spliced Images. IJACSA) International Journal of Advanced Computer Science and Applications, 7(3).