ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

Image Blind Detection Using GLCM, ABC and Voting Classification Method

[1] Kanika, [2] Dr. Vivek Thapar, [3] Er. Gurjit Kaur
[1] Student, GNDEC, Ludhiana, India.
[2] [3] Assistant Professor, GNDEC, Ludhiana, India

Abstract: The image processing tool has attained a lot of attention. Thus, people are capable of manipulating the digital image in quick and easy manner without any obvious traces. The integrity and authenticity of digital images must be determined. The forgery is generated in two ways namely copy-move and splicing. The image blind detection has various phases which include pre-processing, feature extraction and classification. In this research work, GLCM algorithm is used for the textural feature extraction. The artificial bee colony algorithm is applied which can optimize the detected forgery pixels. The hybrid classification method is used for the classification. The hybrid classification method will be the combination of KNN, SVM and decision tree. It is expected that accuracy, precision and recall will be improved for the image blind detection.

Keywords: Image Blind, ABC, GLCM, KNN, SVM, Decision Tree

I. INTRODUCTION

Image processing comes under the family of signal processing. This approach takes the input in form of image and provides the output as an image or a group of attributes regarding the input image. Image processing is considered as an integral discipline of electrical engineering and computer science. Various image processing methods consider the images as 2-D signals and they make the implementation of existing signal processing methods to these images. Thus, the image processing is often recognized as the DIP (Digital Image Processing). But, a few other kinds of image processing schemes are also available like optical and analogue. The computer algorithms are utilized in DIP to process the digital image [1]. At present, digital image is one of the most important carriers helping people to obtain enormous volume of information. Indeed, an image equals immeasurable word. This means that there is tremendous information included in the images. The most common methods for image manipulation are digital image frauds, blurriness, and composition. Digital image forensics has become an important are of research for its applications in validity or detecting forged digital imagery. The objective of digital image forensic studies is to authenticate the validity of digital images and to discover the tampering functions implemented to them by retrieving every information concerning their past. The rapidly growing devices to acquire digital images (such as digital cameras, scanners etc.) have spread the digital images throughout the world. Now, users with the help of cost-free or inexpensive computer tool like paint, photoshop, Picasa can manipulate digital images effortlessly [7]. This results in the manipulation of numerous images, specifically composite forged images which are being appeared in many domains, for example, legal proof, political actions, technical experimentation, educational research, and newspapers. Digital forgery is an operation generally applied to eradicate visible signs of tampering that naked eye can notice. Therefore, there is the need of some algorithms to validate digital images and to detect manipulated images. Fraudsters usually apply two means to perform image forgery, i.e., copy move and splicing. The splicing aims to cover some unnecessary part in the same image by copying a part of a picture and later pasting it over other parts. Verifying discrepancies of certain properties, values, or attributes within the target image are the main steps involved in the detection of a spliced picture. Copy-move refers to a robust form of forgery. Copy move forgery is usually done to hide facts. For example, CMF hides, repeats, or moves the object in the image. It can visually conceal duplicate field components such as color and light by copying it from the same image [8]. There are several factors that must be considered while developing a copy-move forgery detection (CMFD) method. First of all, CMFD must be able to provide highly accurate and reliable detection results. However, the developed technique is also required to be effective in the context of speed and computational intricacy in real-time. Therefore, at present, it is quite challenging to provide solution to the problems concerning speed-accuracy trade-offs. In addition, a

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

competent copy move forgery detection method must be strong against a variety of attacks and tempering schemes. Figure 1.1 represents the general architecture of CMFD.

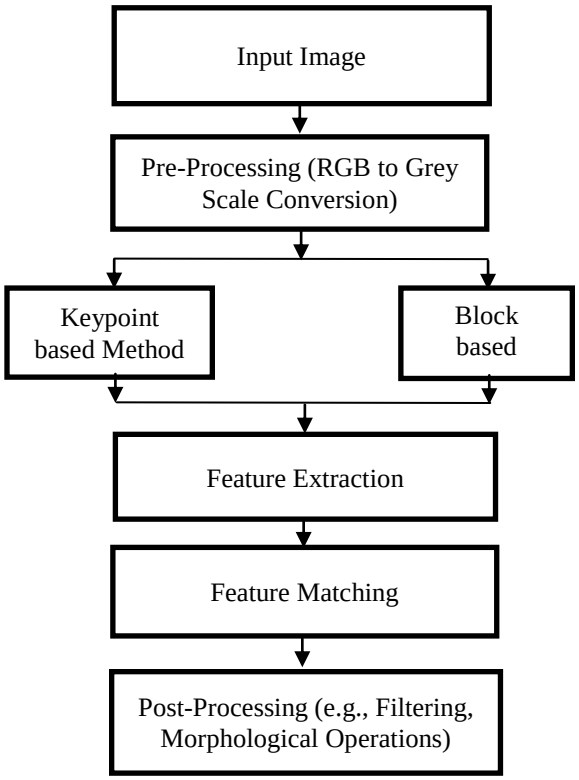

Figure1.1: Framework of CMFD

The steps included in the above structure are discussed below:

a. Pre-processing: This is the initial phase that makes the execution of some conversion, transform or decomposition methods [9]. The pre-processing phase focuses on preparing and revealing the data in a way using which the subsequent feature extraction phase becomes more effective. The most simple and imperative techniques of pre-processing are grayscale conversion that are implemented to transform the RGB pixels into a grayscale image from a range of 0 to 255 and the RGB image is converted to HSV using colour space conversion. This phase also comprises the decomposition methods known as wavelet decomposition or PCA.

Image pre-processing involves the transformation and dimensionality reduction methods, as well as, the block division and segmentation (eg. SLIC). The target digital image is divided into permanent or varying size blocks, sub-blocks, patches, or super pixels using these methods. Figure 1.2 illustrates the framework of the pre-processing phase which consists of two principal elements: Transformation or dimensional reduction-oriented and segmentation-oriented modules.

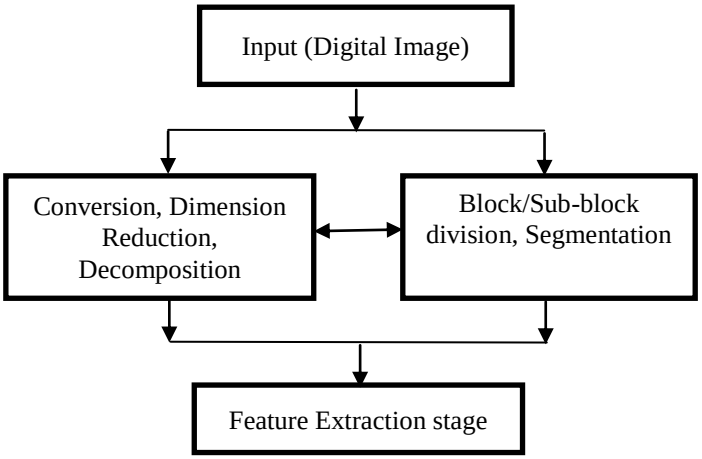

Figure 1.2: Major Units of the CMFD pre-processing phase

In this phase, the sequence of tasks is substitutable and it is possible to visit/perform each unit many times. For example, pre-processing can begin by splitting the target image into square blocks of permanent magnitude and then performing wavelet decomposition (example: DWT) on every single block. Furthermore, based on the architecture and fundamental feature extraction scheme or algorithmic approach, the division of every image block can be done into several sub-blocks [10].

b. Feature Extraction: This phase is executed later on. Feature extraction is the most crucial phase assists in determining the entire accuracy of the system. A set of short but significant data vectors is generated for exposing every portion of the destination digital image. This step aims to generate feature descriptors from each block or keypoint achieved from earlier methods. These descriptors refer to vectors obtained from image data, which have a high degree of discriminatory strength. Thus, the original and the duplicated image in copy move forgery is required to produce a group of feature descriptors that is analogous or almost associated with each other. Each descriptor generated by a powerful extraction method will be highly discriminative in nature which will ultimately be depicted in the total accuracy of the detection framework.

This step is one of the important factors in determining the processing speed of the system, not only to determine the overall detection accuracy [11]. Practically, a single image, specifically a high-resolution image contains

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

multiple key points or blocks. Therefore, it is not an easy to task to prepare feature descriptors for all blocks/key-points. In practice, forensic investigations where the validity of all digital images must be authenticated, the detection speed must be so fast that there is no obstruction, and subsequent investigation procedures should be allowed to run easily. Since the feature extraction process is an important step and serves as the main unit of the copy move forgery detection framework, a large number of research studies have been reported in the literature.

c. Feature matching: This phase includes the discovery of similar feature vectors. For constraining the range of same feature vectors, sorting algorithm are applied to make the similar attributes adjacent and sorted in lexicographical and radix manner [12]. Moreover, the process to investigate the similar feature vectors is enhanced using locality-sensitive hashing (LSH). Several techniques are available for quantifying the similarity among the feature vectors like Euclidean distance and Manhattan distance that have correspondence with Eq. (1) and Eq. (2).

$$d_{Euclidean} = \sqrt{\sum_{i=1}^{n} [v_1(i) - v_2(i)]^2} \dots\dots (1)$$

$$d_{Manhattan} = \sqrt{\sum_{i=1}^{n} |v_1(i) - v_2(i)|} \dots\dots (2)$$

In these equations, v_1 and v_2 are n-dimensional feature vectors. The methods of Feature matching belong to either one of the two types. i.e., searching-based methods and similarity measuring methods. Some of the popular searching-based methods are discussed as following:

i. Sorting: Sorting is a popular method commonly implemented in CMFD techniques. Matching between all descriptors turns out to be computationally difficult since a huge number of feature descriptors are mined from a digital image, specially from high-resolution images. Hence, sorting is generally used to increase the speed of the matching process [13].

ii. Hashing: Hashing is an approach that digests feature descriptors in a smaller and simpler manner. There is a possibility to improve the matching process considerably by comparing the digested descriptors roughly.

iii. Clustering and segmentation: The popularity of this approach is growing fast in this feature matching method of copy move forgery detection. Segmentation (example: SLIC) can be used to split the target image into expressive super pixels/patches. Matching between patches has proved to be highly competent in the context of both accuracy as well as speed as the two descriptors would only be matched between descriptors from dissimilar patches.

iv. Nearest neighbor-based methods: Nearest Neighbor (NN)-based methods are prevalent schemes commonly used in copy move forgery detection [14]. The two nearest neighbor (2NN) technique computes the ratio of the distance between the first and second nearest neighbors (NN). Therefore, the two characteristics are considered a match if the ratio of the distance between the first and second nearest neighbour is below the already defined threshold. The 2NN method is typically carried out by some basic similarity measuring techniques (i.e., Euclidean distance).

In the course of searching, the matching algorithm searches for nearest or almost nearest neighbors to seek out possible matches. Similarity measuring methods act as the basic schemes employed for actually comparing a pair of descriptors. Euclidean distance is surely the modest and most common method in accordance to the recently carried out works.

d. Localization and post-processing: This is the last phase in which filtering and processing of raw matched detection results was carried out for improving and generating the final detection results with the highest quality [15]. In case, the regions that the feature matching determined are represented in the map, various isolated points and morphologic operations, filtering or random sample consensus (RANSAC) algorithm are implemented for the refinement of detected regions. Localization is not a necessary step in the structure of CMFD process that includes visualization of the detection results. Typically, a binary image (i.e., black and white image), making the detected CMF area within the target image visible, is used to generate the detection output.

II. LITERATURE REVIEW

H. Kasban, et.al (2020) stated that the major intend was to present an approach to detect the forgery in digital image [23]. This approach was capable of sensing any small image tampering and robust to image manipulation attacks. Initially, the RGB image was transformed into YCbCr space in this approach. Subsequently, the extraction of Hilbert–Huang Transform (HHT) attributes

was done from the Cr. The image was categorized as genuine or fake by testing and comparing three diverse classification algorithms namely SVM, KNN and ANN. The SSIM parameter was utilized to determine the outcomes so that the DR of forgery was computed. The outcomes depicted that Support Vector machine (SVM) provided a greater precision in contrast to other algorithms.

TinggeZhul, et.al (2019) presented a forgery detection technique on the basis of LBP residue classes and color regions [21]. The partition of an image was done into overlapped blocks. The evaluation of LBP residue classes was performed for every block. The plane generated through 'a' dimensional and 'b' dimensional from Lab color space was split into sixteen regions. The similar LBP residue class and color region had employed to investigate the same blocks and their grouping was performed into various regions later on. At last, the tampered areas were located by analyzing the multi-region relation of these suspicious regions and their areas. The experimental outcomes exhibited that the presented technique performed efficiently in enhancing the DR and mitigating the execution time even under different challenging conditions. This technique had potential to decrease the search range for same blocks. Thus, it provided the greater speed as compared to exhaustive search and comparative detection results simultaneously.

Navdeep Kanwal, et.al (2019) discussed that the methods of forgery detection executed into 2 domains of image forgery: CMFD and ISD [22]. A detailed comparative analysis was carried out to make the utilization of local texture descriptors such as LBP and LTP in detecting the forgery of an image. A method was also put forward for the incorporation of FFT with local texture descriptors so that the image forgery was detected with the help of traditional block-based method. The CASIAv1.0 data set was employed for testing the performance of utilized method and descriptors. Different standard detection parameters like precision and recall were considered to compute the outcomes.

Youssef William, et.al (2019) suggested the forgery image detection methods for two common image tampering methods [24]. The match points methodology was implemented when the attributes were extracted through SIFT and SURF. The splicing was detected by extracting the edges of the integral images of Y, C b, and C r image components. Gray Level Co-occurrence Matrix (GLCM) was executed for every edge integral image and the feature vector was constructed. Afterward, the Support Vector machine (SVM) classification algorithm made the utilization of feature vector. The outcomes demonstrated that the efficiency of SURF over Scale-invariant feature transform (SIFT). The accuracy to detect the tempered images was obtained about 80%. Additionally, the finest outcomes were obtained while detecting the splicing image when the image was processed in YC b C r color model. The TPR was computed 99% in the detection of splicing images.

G. Nirmala, et.al (2019) established a passive technique for recognizing the CMF. The forgery was detected by decomposing the image and extracting the moments as feature vector [30]. The outcomes of experiment indicated that the forgery was detected and the related forged mages were categorized as clusters using the established technique on the basis of hierarchical technique for which BIRCH algorithm was utilized. The images were post processed to recognize the genuine image.

Na Huang, et.al (2018) designed a CNN framework for understanding the derived attributes from each convolutional layer and detecting several kinds of image tampering by the means of automatic feature learning [29]. The CASIAv1.0 publicly available dataset having authentic images and splicing images was employed to conduct the experiments. The modification of this dataset included the retouching images and re-compressing images as the training data. The results proved that the designed framework was efficient and adaptable.

Navya Sara Monson, et.al (2017) introduced a FD approach in which fine inconsistencies were utilized in the color of the lighting of images [25]. This approach was based on ML that employed a behaviour knowledge space. The images which had two or more people were deployed in this approach. The forgery was detecting by combining the complementary illuminate estimators on image regions of similar material. These illuminate estimates assisted in extracting the attributes based in color, texture and edge. Later on, these attributes were used in ML to make the decision automatically.

Khizar Hayat, et.al (2017) recommended a technique to detect the forgery on the basis of DWT and DCT so that the attributes were mitigated [26]. The individual blocks were achieved when the discrete wavelet transform (DWT) image was split. These blocks were deployed in the discrete cosine transform (DCT). Afterward, the comparison of blocks was done on the basis of correlation coefficients. The recommended technique was tested by constructing a tampering method based on mask. This technique provided superior outcomes to other techniques.

GonapalliRamu, et.al (2017) intended a technique in

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

which Scale-invariant feature transform (SIFT) algorithm was utilized. This technique had robustness and less complexity. The matched regions were extracted using the RANSAC algorithm [27]. The results of experiment demonstrated that the intended technique was capable of generating exact results in contrast to traditional technique utilized to detect the forgery. In addition, the features were matched and the tampered region was extracted applying Random Sample Consensus (RANSAC). The accuracy obtained on dataset that included eighty images was evaluated 98%.

Amira Baumy, et.al (2017) focused on implementing the high-pass filtering and histogram equalization as pre-processing phases for supporting the details of the images prior to detect the forgery [28]. A higher precision was obtained for classification using the detail reinforcement procedure. The Illumination histogram was estimated following the pre-processing. The peak value of the histogram derivative was considered as a parameter to detect the forgery. This paper also made the execution of thresholding approach. The classification was performed using the PDFs of the histogram derivative peaks.

III. RESEARCH METHODOLOGY

The proposed algorithm detects the blind and non-blind image. The proposed algorithm is divided into three phases. In the phase 1, the images are taken as input which need to be classified. The whole image is divided into blocks and overlapping blocks are extracted. Then the clustering technique is applied which can cluster the similar type of blocks. In the second phase, the feature extraction process is done with the eigen vector technique. In the last phase, the ensemble classification algorithm is applied for the classification of blind and non-blind faces.

The image blind detection technique has various steps which are explained below:

1. Data Input and Feature Extraction: The dataset of the image blind detection is taken as input from the kaggle. The GLCM algorithm is applied which can extract textural features of the input image. GLCM computations are often deployed for capturing the 2nd order statistics of image textures. The number of co-occurring intensity pairs is computed to evaluate the GLCMs over a selected image region. The fixed angle and offset values are applied to describe the locations of the co-occurring pixels. The spatial association is defined among each pixel and its neighbouring pixels using this statistical approach. GLCM is often executed in the field of texture analysis. The homogeneity, energy, correlation, and contrast are some statistical values whose extraction is done from the co-occurrence matrix.

2. Apply Artificial Bee Colony: The extracted features which are given as input to PCA algorithm for the feature reduction are optimized using artificial bee colony. The ABC algorithm is a kind of swarm intelligence optimization algorithm inspired by bee's behaviour of collecting honey in nature. Compared with other intelligent algorithms such as genetic algorithm and particle swarm algorithm, ABC algorithm has the advantages of low complexity, strong robustness, less set parameters and strong optimization ability.

3. Classification: The extracted features will be given as input to the classification method for the classification which can classify data into blind or non-blind image. In this research work voting classification method is applied which is the combination of KNN, SVM and decision tree. A Voting Classifier is a ML (machine learning) model implemented to train an ensemble of numerous models and predict an output (class) on the basis of their highest probability of chosen class as the output. The findings of each classifier are aggregated and passed into Voting Classifier and the output class is predicted on the basis of the highest majority of voting using this algorithm. Rather that developing the separate dedicated models and investigating the accuracy for each them, a single model is constructed whose training is done with the deployment of these models and the output is predicted on the basis of their combined majority of voting for each output class.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

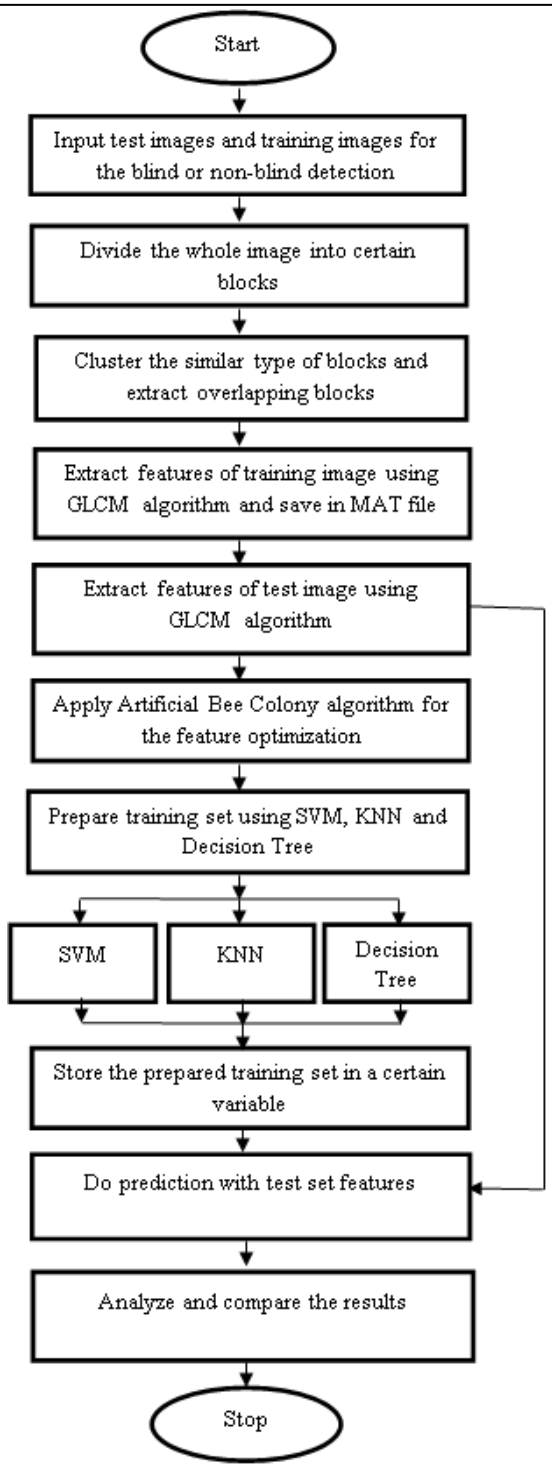

Figure 3.1: Proposed Methodology

IV. RESULTS AND DISCUSSION

This research uses MATLAB software for computing the complex mathematical problems. MATLAB is the software which assists in analyzing the performance of the introduced cache based WSNs. MATLAB is a kind of package using which numerical computations such as addition and subtraction etc. can be done and complex functions can be executed such as technical-computation, graphics and animation. C language is employed as the programming language to simplified MATLAB. An interactive environment having numerous in-built functions is offered by it. These functions are varied from version to version. The matrix is the basic building block of MATLAB. Furthermore, this platform has in-built tools which are image-processing, signal processing, communications, control system and NN (neural networks). These toolboxes can easily perform many functions. Algorithm implementation, graph plotting and the designing of many user interfaces are some of the task performed by this software. This research work uses the datasets from Image communication laboratory for computation purpose. This dataset comprises 2800 original and tampered images. The dataset is available at: \\http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/

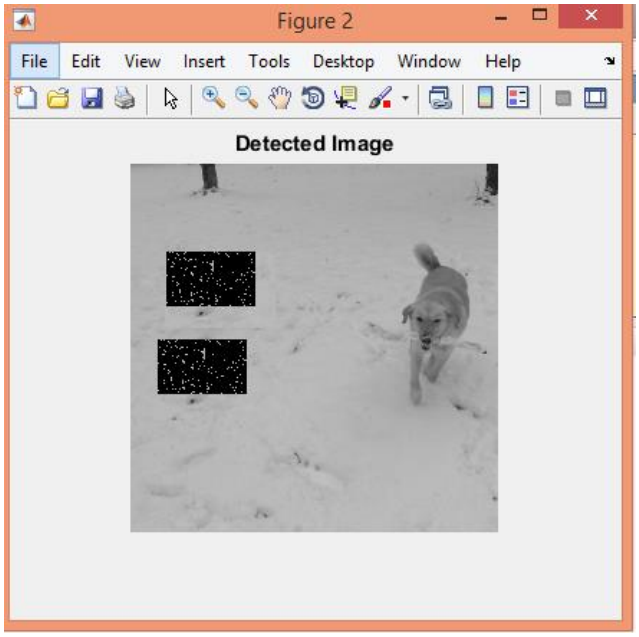

Figure 4.1: Output image with detected forged areas

Figure 4.1 represents the detected regions by marking them with black color.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

Table 1 represents parameter analysis of existing method and the proposed method.

Parameter	Existing Algorithm	Proposed Algorithm
Precision	90 percent	99 percent
Recall	91 percent	99 percent
Accuracy	89 percent	96 percent

Table 1: Parameter Analysis

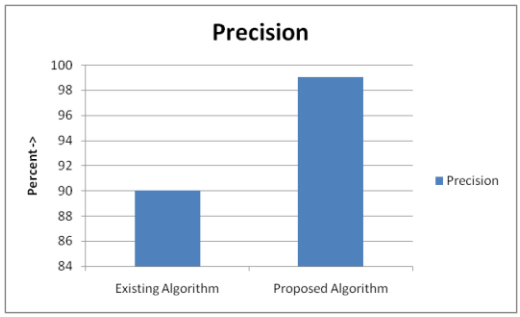

Figure 4.2: Precision Analysis

As shown in figure 4.2, the precision value of existing and proposed method is compared for the performance analysis. The precision value of existing algorithm is 90 percent and proposed algorithm is 99 percent.

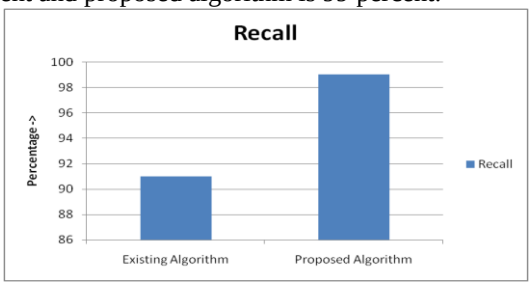

Figure 4.3: Recall Analysis

As shown in figure 4.3, the recall value of existing and proposed method is compared for the performance analysis. The recall value of existing algorithm is 91 percent and proposed algorithm is 99 percent.

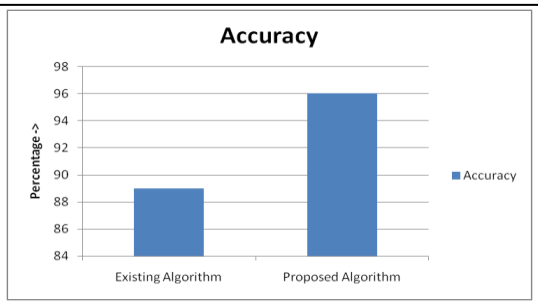

Figure 4.4: Accuracy Analysis

As shown in figure 4.4, the accuracy value of existing and proposed method is compared for the performance analysis. The accuracy value of existing algorithm is 89 percent and proposed algorithm is 96 percent.

CONCLUSION

Image processing comes under the family of signal processing. This approach takes the input in form of image and provides the output as an image or a group of attributes regarding the input image. Image processing is considered as an integral discipline of electrical engineering and computer science. CMFD must be able to provide highly accurate and reliable detection results. The developed technique is also required to be effective in the context of speed and computational intricacy in real-time. Therefore, at present, it is quite challenging to provide solution to the problems concerning speed-accuracy trade-offs. The technique of GLCM is applied which can extract features of the image. The technique of artificial bee colony is applied which can optimize the calculated features. To classify image into blind and non-blind technique of classification is applied which is the combination of SVM, KNN and decision tree. The proposed method is implemented in MATLAB and results are analysed in terms of accuracy, precision and recall. The accuracy for the image blind detection is achieved till 92 percent.

REFERENCES

[1] X. Kang, and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", 2008, in International Conference on Computer Science and Software Engineering, volume 3, issue 10, pp. 92630.

[2] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," 2008, in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, volume 2, issue

15, pp. 2726.
[3] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWTand SVD," 2007, in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, volume 23, issue 15, pp. 17503.
[4] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," 2011, in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), volume 12, issue 4, pp. 14.
[5] I. Amerini et al., "A SIFT-based forensic method for copymove attack detection and transformation recovery", 2011, IEEE Trans. Inf. Foren. Sec., volume 6, issue 3, pp. 1099111
[6] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," 2003, in Proceedings of the Digital Forensic Research Workshop, volume 17, issue 3, pp. 58.
[7] A. C. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," 2004, Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, volume 5, issue 2, pp.34-40
[8] Parul sharma, Harpreet Kaur, "Copy-Move Forgery Detection with GLCM and Euclidian Distance Technique in Image Processing", 2019, International Journal of Recent Technology and Engineering (IJRTE), volume-8, issue- 1C2, pp. 43-47
[9] M. AlSawadi, G. Muhammad, M. Hussain and G. Bebis, "Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering",2013, Modelling Symposium (EMS), volume 5. issue 13, pp. 249-254
[10] H. Yao, T. Qiao, Z. Tang, Y. Zhao and H. Mao, "Detecting CopyMove Forgery Using Non-Negative Matrix Factorization," 2011, Third International Conference on Multimedia Information Networking and Security, volume 8, issue 18, pp. 591-594.
[11] Yanjun Cao, T. Gao, and Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", 2012, Forensic Int., volume 214, issue 7, pp. 33-43
[12] Salam A.Thajeel, Ghazali Sulong, "A Survey of Copy-Move Forgery Detection Techniques", 2014, Journal of Theoretical and Applied Information Technology, volume 70 issue 1, pp. 25-35
[13] Saba Mushtaq and Ajaz Hussain Mir, "Image Copy Move Forgery Detection: A Review", 2018, International Journal of Future Generation Communication and Networking, volume 11, issue 2, pp.11-22
[14] Chengyou Wang, Zhi Zhang and Xiao Zhou, "An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features", 2018, Symmetry, volume10, issue 706, pp. 1-20
[15] Younis E. Abdalla1, M. Tariq Iqbal and M. Shehata, "Copy-Move Forgery Detection Based on Enhanced Patch Match", 2017, International Journal of Computer Science, volume 14, issue 6, pp. 1-7
[16]K Sudhakar, V. M. Sandeep, Subhash Kulkarni, "Speeding-up SIFT based copy move forgery detection using level set approach", 2014, International Conference on Advances in Electronics Computers and Communications
[17] Ghulam Muhammad, Muhammad Hussain, Anwar M. Mirza, George Bebis, "Dyadic wavelets and DCT based blind copy-move image forgery detection", IET Conference on Image Processing (IPR 2012)
[18] Güzin Ulutaş, Mustafa Ulutaş, Vasif V. Nabiyev, "Copy move forgery detection based on LBP", 2013, 21st Signal Processing and Communications Applications Conference (SIU)
[19]Hieu Cuong Nguyen, Stefan Katzenbeisser, "Detection of Copy-move Forgery in Digital Images Using Radon Transformation and Phase Correlation", 2012, Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing
[20] S. A. Fattah, M. M. I. Ullah, M. Ahmed, I. Ahmmed, C. Shahnaz, "A scheme for copy-move forgery detection in digital images based on 2D-DWT", 2014, IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS)
[21] TinggeZhul, Jiangbin Zheng, Yi Lai, Ying Liu, "Image blind detection based on LBP reside classes and color regions", 2019, PLoS ONE
[22] Navdeep Kanwal, Akshay Girdhar, Lakhwinder Kaur, Jaskaran Singh Bhullar, "Detection of Digital Image Forgery using Fast Fourier Transform and Local Features", 2019, International Conference on Automation, Computational and Technology Management (ICACTM)
[23] H. Kasban, Sabry Nassar, "An efficient approach for forgery detection in digital images using Hilbert–Huang transform", 2020, Applied Soft Computing
[24] Youssef William, SherineSafwat, Mohammed A.-M. Salem, "Robust Image Forgery Detection Using Point Feature Analysis", 2019, Federated Conference on Computer Science and Information Systems (FedCSIS)
[25] Navya Sara Monson, K.V. Manoj Kumar, "Behavior knowledge space-based fusion for image forgery detection", 2017, International Conference on Inventive

Communication and Computational Technologies (ICICCT)
[26] Khizar Hayat, Tanzeela Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms", 2017, Computers & Electrical Engineering
[27] GonapalliRamu, S. B. G. Thilak Babu, "Image forgery detection for high resolution images using SIFT and RANSAC algorithm", 2017, 2nd International Conference on Communication and Electronics Systems (ICCES)
[28] Amira Baumy, Mahmoud Abdalla, Naglaa F Soiliman, Fathi E. Abd El-Samie, "Efficient implementation of pre-processing techniques for image forgery detection", 2017, Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)
[29] Na Huang, Jingsha He, Nafei Zhu, "A Novel Method for Detecting Image Forgery Based on Convolutional Neural Network", 2018, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
[30] G. Nirmala, K. K. Thyagharajan, "A Modern Approach for Image Forgery Detection using BRICH Clustering based on Normalised Mean and Standard Deviation", 2019, International Conference on Communication and Signal Processing (ICCSP)
[31] Yang Wei, Xiuli Bi, Bin Xiao, "C2R Net: The Coarse to Refined Network for Image Forgery Detection", 2018, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)