IMPROVED COPY MOVE FORGERY DETECTION AND CLASSIFICATION BY ARTIFICIAL BEE CLONY APPROACH WITH KERNEL METHODS

Mr. BALBIR KUMAR[1] Ms. ANUDEEP GORAYA [2]
[1, 2] ELECTRONIC AND COMMUNICATION ENGINEERING
RAYAT INSTITUTE OF ENGINEERING AND INFORMATION TECHNOLOGY
INDIA

Abstract- **The algorithm of copy-move forgery detection and the steps of processing implements best methodology in various post-processing scenarios. They usually achieve this by the process of casting existing algorithms in a common pipeline. This work suggests the use of two of the following aspects, where first is detection and second one is classification. In case of detection process it shows that which part is copied in the image itself. Whereas in case of classification, it calculates precision, recall and accuracy at its testing phase. In both the sections, the features forms the most significant aspect of the system. In the proposed approach, block base is optimized and key point features are optimized by artificial bee colony approach which help in optimizing the area where the process of feature identification and matching is done and efficient results are compared with the existing approaches. In the methodology of classification learning process, such features with the help of SVM base kernel approach improves the precision, recall and accuracy of the system**

Keywords- Copy move forgery, Ant bee colony,

I. INTRODUCTION

In the era of digital images, it is possible to have tampering effect. Rapid advancement in various techniques helps attackers to modify the contents of digital images. The intelligent use of digital image editing software is constantly increasing the difficulty in distinguishing the authentic image from the tampered one. In copy-move tampering the portion of an image region is copied and moved at a different location of the same image. Splicing is a special case of copy move tampering where copied portion of one image is pasted on some location of different image. Copy-Move is done with the intention either to cover truth or to make some enhancement in the visual effects of the image [1][13]. The copy-move tampering can be performed in a credible manner without much difficulty but the copy-move tampering can be practically difficult to detect. Therefore, it is likely that this kind of tampering can be often applied to forge an image. In courts of law, where images are presented as basic evidence, its verification plays a crucial role as images can be edited to change its meaning and thus influence the judgment. Many prominent personalities of film industry have also been victimized by image tampering. It has begun such an era where seeing is no longer believing [2]. It is thus important to prove the authenticity of the image and bring the truth towards the world. The digital image forensics can be broadly classified into three branches as Image source identification, Computer generated image identification and Image forgery detection. The image forgery detection techniques can again be classified into many categories like, geometry-based technique, format-based technique, camera-based technique, physics-based technique and pixel-based technique. Many tools are available for doing the copy move in Photoshop, proliferation digital cameras, digital signatures, watermarking etc. Copied areas are usually textured regions [6][7]. Thus, it is very much important to have a detection system that automatically identifies the copied move forgery areas, because it may hide some important details and can even change the contents of the image.

1.1 Digital Image Forgery Attack

In this era due to presence of low-cost and high-resolution digital cameras, there is wide number of digital images all over the world. Digital images play a very important role in areas like forensic investigation, insurance processing, surveillance systems, intelligence services, medical imaging and journalism. But the basic requirement to believe what we see is that the images should be authentic [3] [4]. With the availability of powerful image processing software's like Adobe Photoshop it is very easy to manipulate, alter or modify a digital image. Any image manipulation can become a forgery, if it changes semantic of original image. [10]. There can be many reasons for a forgery to be occurred by a forger like: To cover objects in an image in order to either produce false proof, to make the image more pleasant for appearance, to hide something in image, to emphasize particular objects etc.

1.2 Types of Digital Image forgery

There are many ways to categorize the digital image forgery, but main categories of Digital image Forgery are Enhancing, Retouching, Splicing, Morphing and Copy/Move. Following is brief description of different types of digital image forgery:

1.2.1 Image Enhancing: Image enhancing involves enhancing an image with the help of Photoshop such as saturation, blur and tone etc. These enhancements don't affect image meaning or appearance. But somehow effects the interpretation of an image [2]. Enhancing involves changing the color of objects, changing time of day in which the image appears to have been taken, changing the weather conditions, Blurring out objects.

1.2.2 Image Retouching: It is basically used to reduce certain feature of an image and enhances the image quality to capture the reader's attention. In this method, image editors change the background, fill some attractive colors, and work with hue saturation for toning.

1.2.3 Image Splicing: In image splicing different elements from multiple images are pasted into a single image. At last, one image is obtained from content of different images.

1.2.4 Image Morphing: Image morphing is defined as a digital technique that gradually transforms one image into another. Transformations are done using smooth transition between two images.

1.2.5 Copy-Move: In copy-move forgery one region is copied from an image and pasted onto another region of the same image. Therefore, source and the destination both are same. Copy Move involves copying regions of the original image and pasting into other areas.

1.3 Copy Move Forgery Attack

Copy-Move is a type of forgery in which a part of image is copied and then pasted on to another portion of the same image. The main intention of Copy-Move forgery is to hide some information from the original image. Since the copied area belongs to the same image, the properties of copied area like the color palette, noise components, dynamic range and the other properties too will be

compatible with the rest of the image [3.5]. So, the human eye usually has much more trouble detecting copy-move forgeries. Also, forger may have used some sort of retouch or resample tools to the copied area so as it becomes even more difficult to detect copy-moved forgery. Retouching involves compressing the copied area, adding the noise to the copied area etc. and re-sampling may include scaling or rotating the image. For example: An image from the crime scene is taken. Fig. 1 shows the original image and figure 2 shows the forged image. Forgery is done to hide some important evidences.

Figure 1: Original Source Image

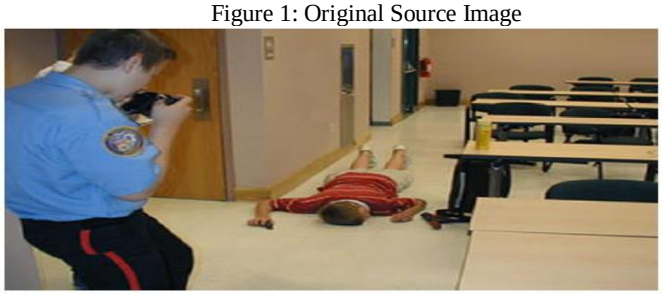


Figure 2: Output Forged Images

1.4 Need for Digital Image Forgery Detection

With the availability of low cost and high-quality digital cameras and easy methods of sharing the digital images, Digital images have become an integral part of almost every area. So, image authenticity and integrity represent a major concern. And there must be techniques to detect whether an image has been forged or not. Authenticity of images can't be taken for granted, especially when it comes to legal photographic evidence [1][5]. Digital images play a very important role in areas. Following are some important areas in which integrity and authentication of a digital image is very necessary:

- Medical images are produced in most of the cases as proof for unhealthiness and claim of disease.
- In courtrooms digital images are used as evidence and proofs against various crimes.
- In e- commerce sites images are an essential component when trying to stand out from the crowd and attract customers.

1.5 Digital Image Forgery Detection Methods

Digital image forgery detection techniques are mainly classified into two categories: one is active approach and other one is passive approach. See figure 3. Active approach requires a pre-processing step and suggests embedding of watermarks or digital signatures to images. It relies on the presence of a watermark or signature and therefore require knowledge original image. So, it limits their operation. Algorithm/key used to embed the watermark or fingerprint. Any manipulation of the image will impact the watermark and subsequent retrieval of the watermark and examination of its condition will indicate if tampering has occurred whereas, **i**n case of passive approach forgery detection, there is no requirement of knowledge of original image [9]. It does not rely of presence of Digital watermark or Digital fingerprint. The passive approach is regarded as evolutionary developments in the area of tamper detection [7][8].

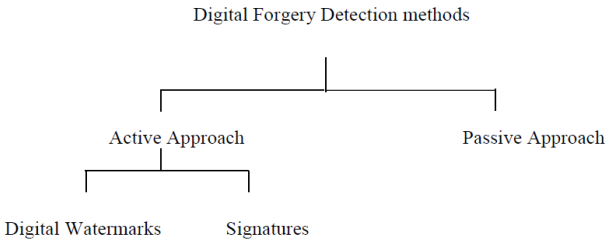


Figure 3: Digital Forgery detection Methods

1.5.1 Active Approach

Active methods require pre-embedded information about image like the source (camera) of the image or the acquisition device used. Digital watermarking and digital signatures are the methods which use active approaches. A digital signature is an external authentication code which is generated from the original message. It is usually an encrypted type of hash values. It incorporates the authentication code which is to be verified and added some other data, for example, the guarantor, the proprietor, and the legitimacy time of people in general key. An open key testament is a digitally marked message which comprises two sections that are utilized for validation utilizing people in general key [12]. Cryptography is a strategy which is utilized for the picture authentication through digital signature. D.S works just when a validation message is transmitted with the media. In this kind of validation digital signatures are put away in the header of organization or in a different document. The significant hazard in this is losing the signature. It doesn't give the security against the unapproved replicating. The complex methodologies of cryptography give the security against this issue yet it is extremely costly.

1.5.2 Passive Approach

The major obstacle in the active image authentication based on digital signature is that a signature must be available for the authentication which limits the explained approach. Passive authentication is an alternate method or active authentication. This method uses the image itself for authentication and integrity of the image without using any related information of the image [11].

II. RELATED WORK

Agarwal, Saurabh, et al. [1] In this paper, the author proposed an image forgery detection using co-occurrence-based Texture operator in frequency domain. Wavelet transforms and texture descriptor method is used for the tempering detection in blind image. Shift-variant method is used to highlight the crucial details of the images. These methods provide more information related to image internal statistics. This information is converted into the feature vector. To distinguish between the image and pristine SVM kernel with linear classifier is used and give effective results. Novozámský, Adam et al. [2] In this work, image compression model is used to detect the image modification. This method is used to overcome the problem of post-processing which is caused by failure of detection. In this method a JPEG constraint is defined and matched with the image constraint. This method improves the detection of image modification and gives effective results. Yang, Bin, et al. [3] This paper describes the copy move forgery detection by using SIFT method. In this work distributing strategy is used for interspersing. SIFT method is used to descripted the key-points and enhanced the detection rate. The result of the proposed method shows the robustness of the approach. Xiang, Ruxi, et al. [4] In this paper, the author proposed big data clustering method for image-forgery detection. This paper proposed matching method which improves the detection accuracy. K-mean clustering method is used to make the clusters of the image blocks. Then it matches the same block in each cluster by using local hash matching method. This method is

based on the Zernike moment approach which reduced the processing time and improves the accuracy in results. Mahmood, T., et al. [5] This paper introduced a forensic approach for expose the region duplication in the digital images. This approach divides the LL sub-band into the overlapping blocks. Features are extracted from the overlapped blocks which expose the forgery in the image. The results of the proposed approach show its effectiveness on the basis of recall, precision and F-score of different blocks. This approach is very helpful in crime investigation and news reporting. Emam, Mahmoud, et al. [6] Two-stage keypoint detection method is used for forgery detection in digital images. This method is proposed to detect the forgery in the smooth region when the changes go sensitivity to geometric. Spatial distributed keypoint are detected by scale invariant feature operator. Missing keypoint from the images is detected by using Harris corner detector with non-maximal suppression. Gradient histogram descriptor is used to match the performance of local features point. The result of the proposed method shows the better detection and robustness from geometric transformation attacks. Abrahim, Araz Rajab, et al. [7] Artificial neural network and texture feature method is used for the splicing image forgery detection in this proposed work. Texture features automatically detect the spliced image by matching the edge of the object and the colours of the object. In this work vectors of the three features are combined and then fed into the ANN classifier and then takes the decision on the basis of features majority. Birajdar, Gajanan K., et al. [8] In this paper, the author proposed an image forgery detection by using feed forward neural network and support vector machine. Fisher approach is used to select the effective features from the image and reduce the dimensionality of the statistical features. This method has also capability to detect the rescaled image detection. The result of the proposed paper shows that Multi-layer ANN work better than ANN with SVM. Emam, M., Han, et al. [9] In this paper, the author proposed a robust algorithm to detect the forgery in the images in smooth regions. This method detects the extreme points from difference of Gaussian operator. This method is use due to its effective approximation for the Laplacian and it is very faster in calculations. Multi-support Region Order-based Gradient Histogram (MROGH) descriptor is used to detect the descriptive features. Results of the proposed work show it robustness in detection. Zhu, Y., et al. [10] In this paper, the author detects the similar but genuine objects in the forged images. This work also investigates the CMFD methods. Feature extraction process is done by using orientation assignment then these features are applied for texture description and then match the features using RANSAC method. This method also reduced the false matched features and then calculates the correlation coefficient of the regions. Yang, F., et al. [11] The author introduced a copy move forgery detection method by using the hybrid features. Matching algorithm is used to find the best features from the all features. False matches of the features are filtered out by using the segmentation process. This process finds the duplicated regions in the image. This method performs better than existing methods and approaches in duplicate region detection. Zhong, J., Gan, et al. [12] In this paper, the author proposed the block-based method for forgery detection under the image geometric transforms. In this work pre-processing of the image then divides the forged image into overlapped circular blocks. Discrete radial harmonic Fourier function is used to extract the inner and local feature from the image. Nearest neighbor method is used to found the similar feature vectors. Isolated features are removed by using Morphological operation. Beste Ustubioglu et al. [13] In this paper authors proposed a method to calculate threshold automatically. Threshold is value that is used to compare similarity between feature vectors. Authors utilize DCT-phase terms to restrict the range of the feature vector elements' and Benford's generalized law to determine the compression history of the image under test. The method uses element-by-element equality between the feature vectors instead of Euclidean distance or cross correlation and utilizes compression history to determine the threshold value for the current test image automatically. Experimental results show that the method can detect the copied and pasted regions under different scenarios and gives higher accuracy ratios/lower false negative compared to similar works.

III. THE PROPOSED METHOD

3.1 Proposed Methodologies

In this design methodology firstly, image is converted into overlapping blocks after converting into grey scale, then features are extracted using Ant colony Optimization, then matching will be performed using Ant colony Optimization and at last forged regions are marked. Steps are as following:

1. Take a colored forged image as input.
2. Convert image into Grey Scale.
3. Divide greyscale image into overlapping blocks.
4. Store these blocks into a metrics.
5. Extract feature vectors using Particle Swarm Optimization. If not optimized the apply ACO otherwise converge and analyse the parameters.
6. Match similar feature vectors using Ant Colony Optimization.
7. Initialize ants.
8. Evaluate results and update pheromone values.
9. Check if exit criteria met.
10. If yes give final detected forged regions, else initialize new ants.

3.2 Proposed methodology: Flowchart

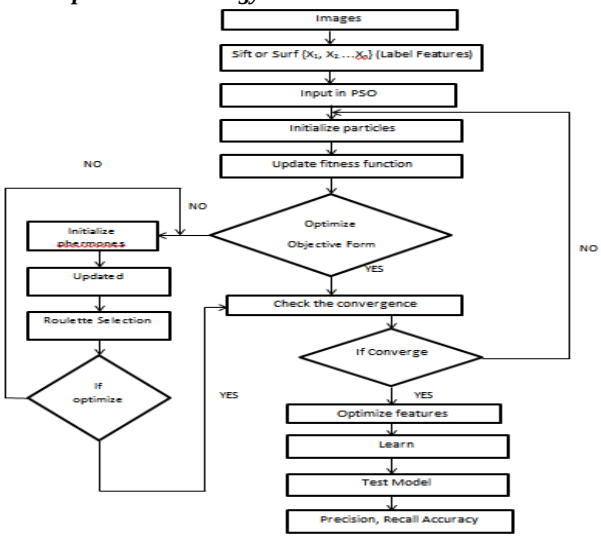


Figure 3: Proposed Flowchart

3.3 Proposed Algorithm

1. Particle Swarm Optimization: PSO is an optimization technique that is based upon bird flocking and fish schooling. Swarm is the collection of particles. There is some objective function whose value has to be optimized with PSO. The optimized value of the objective function will be some point in the search space. Every particle moves in the search space to find the point at which objective function is optimized. At any point of time, every particle has some position and velocity in the search space. Initially, positions and velocities of particles are randomly assigned. After each iteration, positions and velocities of particles are updated using equations 1 and 2. Every particle in PSO has its local best position and the global best position of the swarm. Global best position of the swarm is the position of the particle which is closer to the optimal value. All the particles will

move towards the global best position as it is close to the optimal value. Global best position of the swarm will be updated if some other particle's position becomes closer to the optimal value. Now, this particle's position will become the global best position of the swarm. All the particles will move towards this updated global best position. In this way, at some point of time, all the particles will converge at one point and this point will give the optimal value of the objective function.

$V_{i,d}(t+1) = \alpha\ (t)V_{i,d}(t) + \beta_p ran_p(t)\ (persbest_{i,d}\text{-}P_{i,d}(t)) + \beta_g ran_g(t)\ (globest_d\text{-}P_{i,d}(t))$ (1)

$P_{i,d}(t+1) = P_{i,d}(t) + V_{i,d}(t)$ (2)

Where $V_{i,d}$and $P_{i,d}$is the velocity and position of particle I , dimension d at iteration t+1.α(t) is the weight that tracks the history of velocity, $\beta_p ran_p(t)$ and $\beta_g ran_g(t)$ are the random factors,$persbest_{i,d}$ is the Personal Best of particle I for dimension d and globest is the Global Best of the swarm for dimension d.

2. ACO: Ant Colony Optimization: Ant colony optimization is fundamentally roused by the genuine ant settlements conduct and called artificial framework. Through the charts the Ant colony optimization calculation (ACO) is utilized for the taking care of computational problems and discovering great way. Like ant conduct, looking for way between food source and their colony to look through an ideal way comparative is the principle point of this calculation. To take care of the problem of traveling salesman problem (TSP) the principal ACO was created. Prior to the pheromones are refreshed along their food source trail on change probability bases a probability decision is made in the standard ACO. Before refreshing the pheromones along their trail to a food source in the standard ACO, which depends on the progress probability, ants settles on a probabilistic decision. For the kth ant the change probability at the time step t from city x to city y in the TSP problem:

$$PROB_{xy}^{k}(t) = \begin{cases} \frac{[\tau_{xy(T)}]^{\alpha}.[\eta_{xy}]^{\beta}}{\sum_{y\epsilon I_x^k}[\tau_{xy(T)}]^{\alpha}.[\eta_{xy}]^{\beta}} \text{ if j}\epsilon I_x^k \\ 0 \qquad Otherwise \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Where

η_{xy}←priority heuristic information,

τ_{xy}←pheromones trail amount on the edge (x, y) at the time T,

The pheromone trail and heuristic information relative effects are identified by two factors i.e., $\alpha$and β. And the city's neighborhood set that are reasonable is denoted by I_x^k.

After a visit is finished by every ant, a constant dissipation rate at first bringing down them which refreshed the pheromone trail. Inferable from which every ant is permitted effective pheromone affidavit on curves which is its visit part as appeared in the condition underneath:

$$\tau_{xy} = (1-\rho).\tau_{xy} + \sum_{k=1}^{N}\Delta\tau_{yx}^{k} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Where

ρ←pheromones rate of trail evaporation,

N←no. of ants,

The pheromone trail that is boundless aggregated is averted by the utilization of parameter ρ which empowers the awful choices to be overlooked by the calculation. The no. of cycles declining the pheromone quality related on circular segments which ants don't choose. $\Delta\tau_{yx}^{k}$, the trail substance quality per unit length which lays nervous (y,x) is given as takes after:

$$\Delta\tau_{yx}^{k} = \begin{cases} \frac{Q}{L_k} \ if\ ant\ k\ in\ its\ tour\ uses\ edge\ (y,x) \\ 0 \qquad Otherwise \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Where

Q←constant that is predefined,

L_k←length of the tour.

IV. RESULT ANALYSIS

4.1 Performance Metrics

The following quantitative metrics are used to evaluate the performance of the present work.

(1) Accuracy: Accuracy is the starting point for a predictive model quality analyzing, as well as for prediction obvious criterion. Accuracy measures the ratio of correct predictions to the total number of cases evaluated.

Accuracy = TP+TN / (TP+TN+FP+FN)

Where,

TN is the number of true negative cases

FP is the number of false positive cases

FN is the number of false negative cases

TP is the number of true positive cases

2. Precision: Precision (P) is defined as the number of true positives (T_P) over the number of true positives plus the number of false positives ((F_p).

Precision = TP / (TP+FP)

3. Recall: Recall (R) is defined as the number of true positives (T_P) over the number of true positives plus the number of false negatives (F_n).

Recall = TP / (TP+FN)

4. True positive rate: TPR refers to the positive samples proportion which predicts correctly as shown below:

$$TPR=\frac{TP}{TP+FN}$$

5. False Positive Rate: FPR refers to the false positive rate expectancy. It is calculated as the ratio between wrongly categorized negative case numbers as positive (FP) and actual negative numbers in total.

$$FPR=\frac{FP}{FP+TN}$$

4.2 Detection

Below given figure 4 and figure 5 show the experiment on two types of feature SIFT with ACO and SURF feature but results show SURF features not able to detect forgery part in image but ACO optimization feature detect

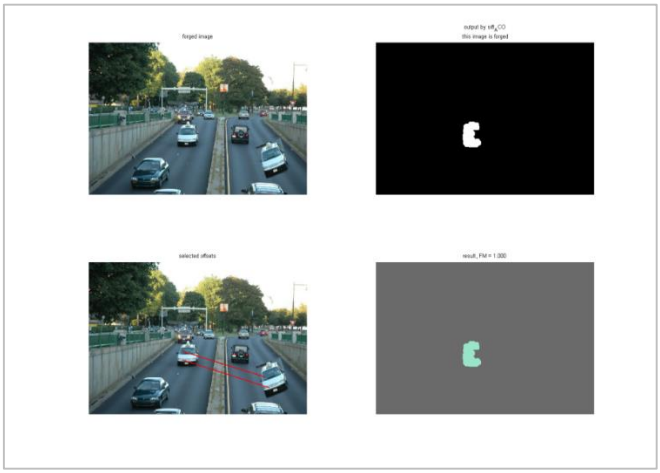


Figure 4: Analysis of SIFT _ABC features Detection

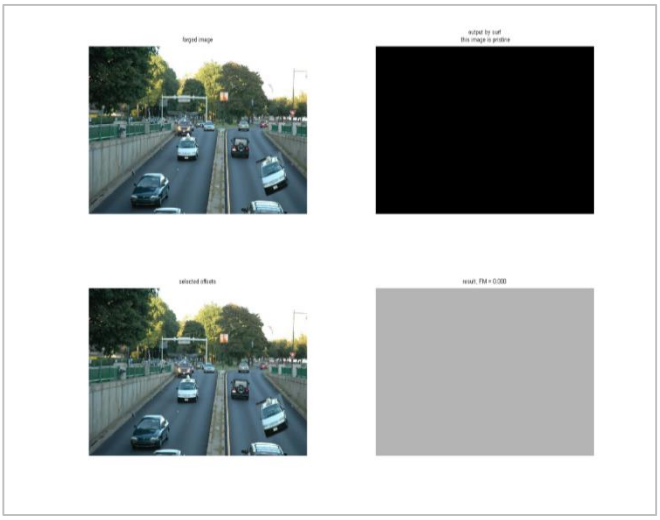


Figure 5: Analysis of SIFT ACO features Detection

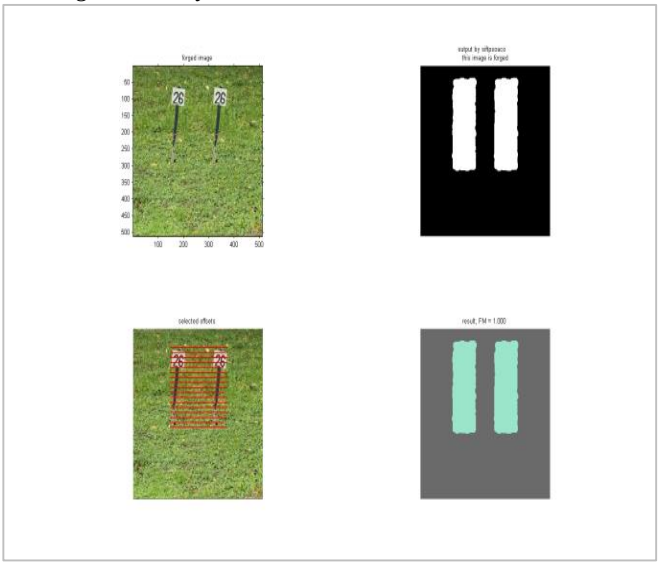


Fig 6 (a) SIF_ABC

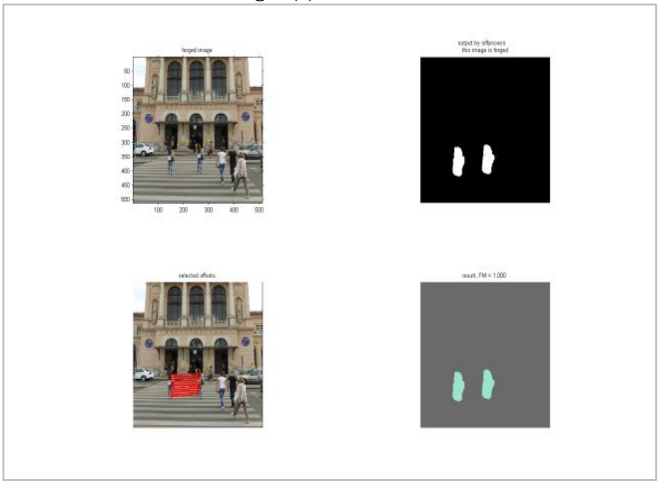


Fig 6 (b) SIF_ABC

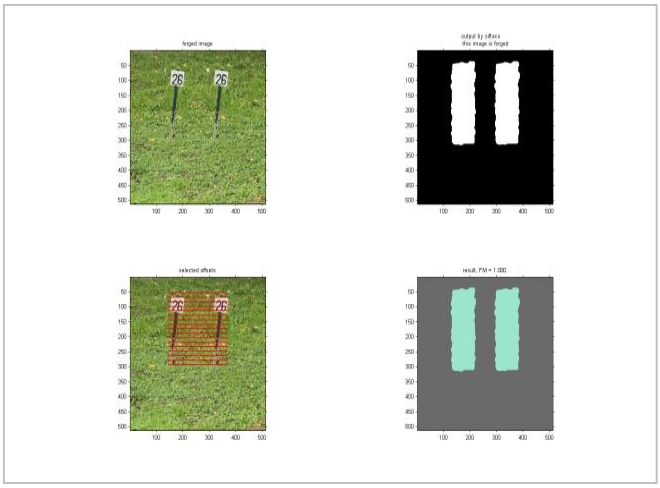


Fig 7 (a) SIF_ACO

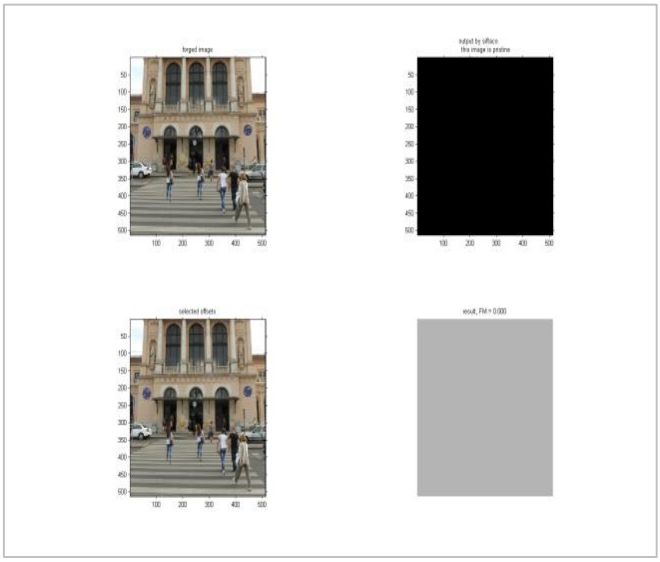


Fig 7 (b) SIF_ACO

4.3 Result Analysis

The following section shows the tales and graphs showing the results of implementation to calculate values of various parameters.

Table 1 Precision Value for Different Classifier

Classifier	Precision
SIFT with ACO (polynomial)	0.8917
Surf (Gaussian)	0.4714
SIFTwith GWO_ABC (Gaussian)	0.9
Surf (polynomial)	0.4737

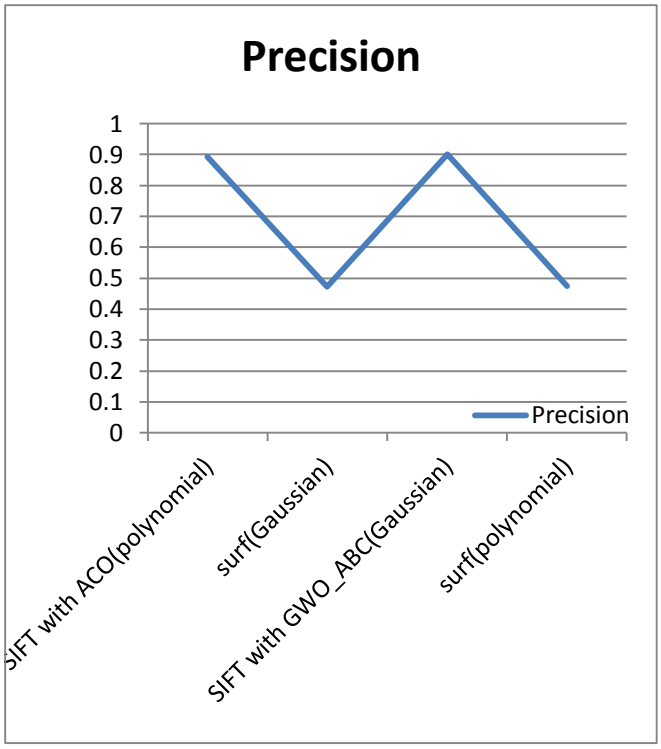


Figure 8: Graph showing the precision for different classifiers

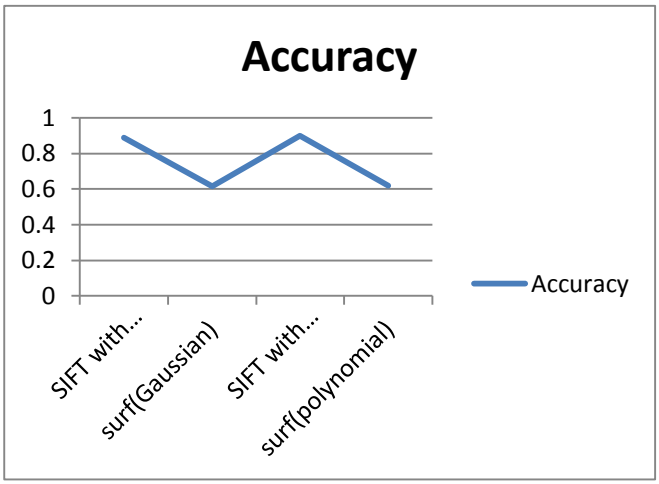
Figure 8 depicts the precision of the four classifiers that are SIFT with ACO (polynomial), surf (Gaussian), SIFT with GWO_ABC(Gaussian) and surf(polynomial). The graph shows the maximum precision is on SIFT with GWO_ABC(Gaussian) classifier and minimum is on surf (Gaussian).

Table 2 Accuracy Value for Different Classifier

Classifier	Accuracy
SIFT with ACO (polynomial)	0.8896
Surf(Gaussian)	0.6153
SIFT with GWO_ABC (Gaussian)	0.8979
Surf(polynomial)	0.6193

Figure 9: Graph showing the accuracy value for different classifiers

Figure 9 depicts the accuracy of the four classifiers that are SIFT with ACO(polynomial), surf(Gaussian), SIFT with GWO_ABC (Gaussian)and surf(polynomial).SIFT with GWO_ABC (Gaussian)



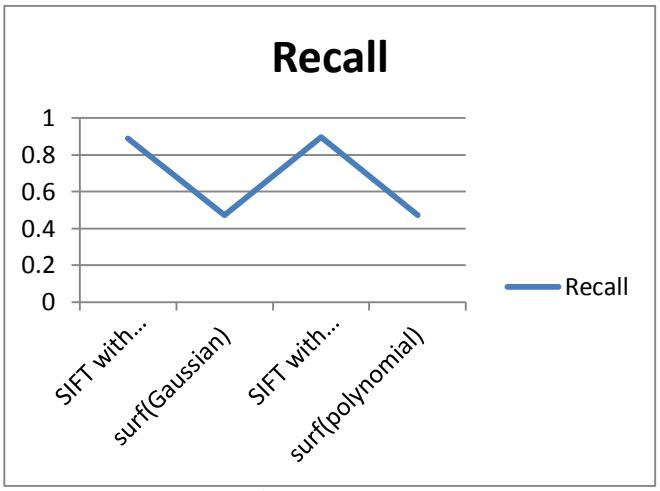
shows the maximum accuracy classifier and minimum is on surf(Gaussian).

Table 4.3 Recall Value for Different Classifier

Classifier	Recall
SIFT with ACO (polynomial)	0.888
Surf(Gaussian)	0.4703
SIFT with GWO_ABC (Gaussian)	0.8963
Surf(polynomial)	0.4726

Figure 10: Graph showing the Recall value for different classifiers

Figure 10 depicts the recall of the four classifiers that are SIFT with PSO (polynomial), surf (Gaussian), SIFT with



GWO_ABC(Gaussian)surf(polynomial). SIFT with ACO(Gaussian) shows the maximum recall classifier and minimum is on surf(Gaussian).

Table 4 Comparison between parameters (Precision, Accuracy, Recall) of different classifiers

Classifier	Precision	Accuracy	Recall

SIFT with ACO(polynomial)	0.8917	0.8896	0.888
Surf(Gaussian)	0.4714	0.6153	0.4703
SIFTwith GWO_ABC (Gaussian)	0.9	0.8979	0.8963
Surf(polynomial)	0.4737	0.6193	0.4726

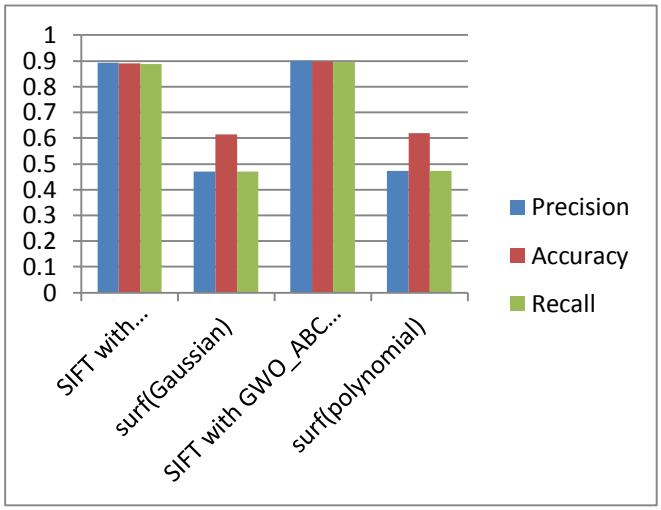


Figure 11 Graph showing the comparison of all the parameters

Figure 11 depicts the precision of the four classifiers that are SIFT with ACO (polynomial), surf (Gaussian), SIFT with GWO_ABC (Gaussian)surf(polynomial). This figure shows the comparison of Precision, recall and accuracy on the different classifiers. The overall good result of the SIFT with GWO_ABC(Gaussian) Classifier.

IV CONCLUSION

Copy-move forgery is a very common way to tamper an image. Many of the researchers have proposed various schemes to detect the tampered images. Sometimes the copied regions are rotated or flipped before being pasted. In this paper, detection and classification methods are done by using the concepts of machine learning along with the use of optimization methods. In the present work, forgery detection and classification is done by using SIFT with ABC and SIFT GWO_ABC with SVM Gaussian and polynomial kernel. The experimental results indicated that the GWO_ABC provides a great significance entailing high accuracy, precision and recall in case of classification processs.

V REFERENCES

[1] Agarwal, Saurabh, and Satish Chand. "Image Forgery Detection Using Co-occurrence-Based Texture Operator in Frequency Domain." *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*. Springer, Singapore, 2018. 117-122.

[2] Novozámský, Adam, and Michal Šorel. "Detection of copy-move image modification using JPEG compression model." *Forensic science international* 283 (2018): 47-57.

[3] Yang, Bin, Xingming Sun, HongleiGuo, Zhihua Xia, and Xianyi Chen. "A copy-move forgery detection method based on CMFD-SIFT." *Multimedia Tools and Applications* 77, no. 1 (2018): 837-855.

[4] Ju Zhu, Yuan Li, and Ruxi Xiang. "Image-based forgery detection using big data clustering." *Multimedia Tools and Applications* (2018): 1-8.

[5] Mahmood, T., Mehmood, Z., Shah, M., & Khan, Z. (2018). An efficient forensic technique for exposing region duplication forgery in digital images. *Applied Intelligence*, 1-11.

[6] Emam, Mahmoud, Qi Han, and Hongli Zhang. "Two- stage Keypoint Detection Scheme for Region Duplication Forgery Detection in Digital Images." *Journal of forensic sciences* 63.1 (2018): 102-111.

[7] Abrahim, Araz Rajab, MohdShafryMohd Rahim, and Ghazali Bin Sulong. "Splicing image forgery identification based on artificial neural network approach and texture features." *Cluster Computing* (2018): 1-14.

[8] Birajdar, Gajanan K., and Vijay H. Mankar. "Subsampling-Based Blind Image Forgery Detection Using Support Vector Machine and Artificial Neural Network Classifiers." *Arabian Journal for Science and Engineering* (2018): 1-14.

[9] Emam, M., Han, Q., Li, Q., & Zhang, H. (2017, July). A robust detection algorithm for image Copy-Move forgery in smooth regions. In *Circuits, System and Simulation (ICCSS), 2017 International Conference on* (pp. 119-123). IEEE.

[10] Zhu, Y., Ng, T. T., Wen, B., Shen, X., & Li, B. (2017, August). Copy-move forgery detection in the presence of similar but genuine objects. In *Signal and Image Processing (ICSIP), 2017 IEEE 2nd International Conference on* (pp. 25-29). IEEE.

[11] Yang, F., Li, J., Lu, W., &Weng, J. (2017). Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence*, *59*, 73-83.

[12] Zhong, J., Gan, Y., Young, J., Huang, L., & Lin, P. (2017). A new block-based method for copy move forgery detection under image geometric transforms. *Multimedia Tools and Applications*, *76*(13), 14887-14903.

[13] Kashyap, A., Agarwal, M., & Gupta, H. (2017). Detection of Copy-move Image forgery using SVD and Cuckoo Search Algorithm. *arXiv preprint arXiv:1704.00631*.

BIBLOGRAPHY