Novel approach of copy forgery detection by swarm intelligence convex optimization

Sonali[1], Ramanjeet kaur [2]
[1, 2] *ECE, Modern Institute of Engineering and Technology*
(Sonali3611269@gmail.com, hod.ece@mietkuk.in)

Abstract-In our society digital images are a powerful and widely used communication medium. They have an important impact on communication and IT industry. the proposed versatile over division calculation sections the host picture into no overlapping and sporadic blocks adaptively. Then, the element focuses are removed from each block as block elements, and the block components are coordinated with each other to find the named highlight focuses; this technique can around show the presumed forgery districts. In past few years, research goes to detecting and classified for copy move forgery images for forensic requirement. So detection is very important challenges for testing in forensic science. In this paper detection and classification by point base and block base features SIFT and SURF Respectively but use hybrid approach of rtificial bee colony with grey wolf optimization (ABC_GWO) in matching and feature selection phases ,in case of SIFT features and proposed SIFT with ABC_GWO features which also use in classification with support vector machine with Gaussian and polynomial kernel.

Keywords- *SIFT,optimization,features; classification.*

I. INTRODUCTION

1.1 Digital Image Forgery Attack

In this era due to presence of low-cost and high-resolution digital cameras, there is wide amount 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]. 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 [9]. 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 [11]. 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 changes the background, fill some attractive colors, and work with hue saturation for toning [11].

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 [9]. 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. 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 fig. 2 shows the forged image. Forgery is done to hide some important evidences.

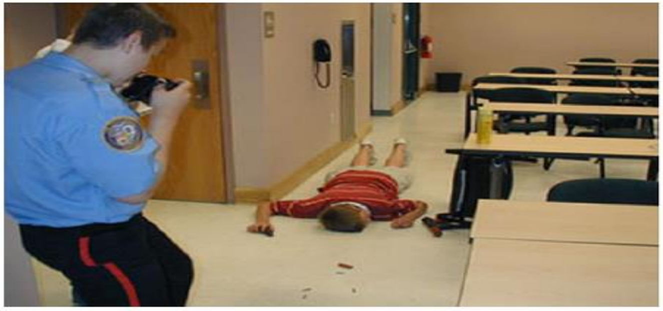

Fig.1:Original Image [3]

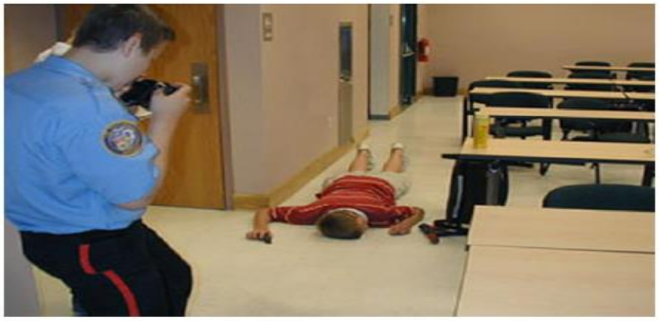

Fig.2: Forged Images [3]

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 is a major concern [11]. 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 [10].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:

A. Medical images are produced in most of the cases as proof for unhealthiness and claim of disease.
B. 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 [2, 16].See figure 3. Active approach requires a pre-processing step and suggests embedding of watermarks or digital signatures to images [16]. 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, in case of passive approach forgery detection, there is no requirement of knowledge of original image. 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 [16].

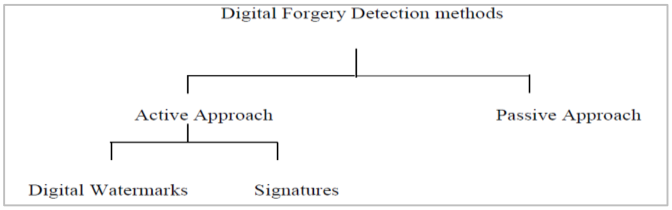

Fig.3: Digital Forgery detection Methods [10]

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 [1, 5]. Digital watermarking [37] 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 [7]. 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. 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.

1.6 Copy Move-Forgery Detection Techniques

A number of methods have been proposed by different authors to detect Copy Move Forgery. All techniques follow a common pipeline to detect the forged areas in an image. The common workflow is shown in figure 4.

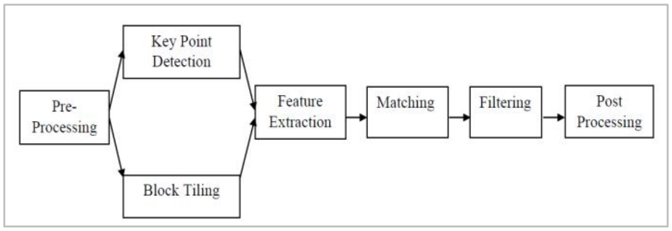

Fig.4 Common processing pipeline for Copy Move Forgery Detection [14]

Methods for detection of copy move forgery has been categorized into two major categories which are as following:

1. Key Point Based detection.
2. Block Based detection.

In Block based method image is divided into several over lapping blocks. The blocks are compared against each other in order to see which blocks are matched. The regions of the image covered by the matching blocks are the copied and forged regions. In case of Key Point Based method no subdivision of image is done. Rather detection is done on the basis of key points found in the image. These key points are the regions with the high entropy. Both methods differ in only feature extraction rest steps are same.

1.6.1Block Based Copy Move Forgery Detection

Block based method splits the image into overlapping blocks and apply a suitable technique to extract features on the basis of which the blocks are compared to determine similarity [1]. Firstly the image is pre-processed i.e. converted to grayscale. Pre-processing is optional. Then the image is subdivided into overlapping blocks of pixels. For an image size of M × N and a block n size of bxb, the number of overlapped blocks is given by (M-b+1) x (N-b+1). On each of these blocks, a feature vector is extracted. After feature extraction matching is done. Feature vector depends on which feature has been used. Highly similar feature vectors are matched as pairs. Methods that are used for matching are lexicographic ordering on the feature vectors and nearest neighbor determination [21]. Any one from both can be used. The similarity of two features can be determined by different similarity criteria, e.g., the Euclidian distance. There are a number of algorithms that according to the features that are selected for the feature extraction.

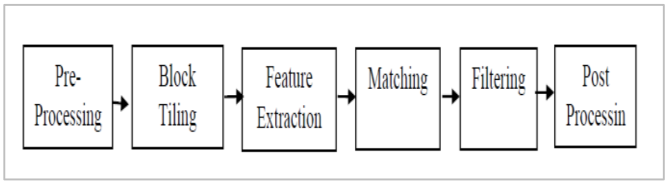

Fig.5: Common processing pipeline for Copy Move Forgery Detection [21].

Following Steps are performed for Copy Move forgery detection:

I Block Tiling: In this step image is divided into n by n non-overlapping blocks.

II Feature Extraction: Feature processing depends on the method used for detection. In case of Block based method there are a number of features like blur, HU, Zernike, Principle Component Analysis, Kernel Principle Component Analysis, etc. which are classified under categories like Moments based , Intensity based, frequency based etc. In case of Key point based method we have lesser features. SIFT and SURF are used mainly to extract local features of images [21].

III Matching: Matching is done to detect the duplicated regions. High similarity between two feature descriptors is interpreted as a cue for a duplicated region. Methods used for matching can be lexicographic sorting, Best-Bin-First search etc. [21].

IV Filtering: There is a high probability that we may get false matches in the previous step, as the copied area comes from the same image. Areas that not have been forged may also be detected as forged. So, after finding the matches filtering is done to reduce the probability of false matches [20].

V Post processing: Post processing is done to detect and preserve matches that exhibit a common behavior. Set of matches that belongs to a copied region are expected to be spatially close to each other in both the source and the target blocks or key points. Furthermore, matches that originate from the same copy-move action should exhibit similar amounts of translation, scaling and rotation [14].

II. ALGORITHM

Ant Colony Optimization: (ACO) studies ant systems and is used to solve discrete optimization problems. Artificial Ant Colony System (ACS) is an agent-based system, which simulates the natural behavior of ants. It is used to find good solutions to combinatorial optimization problems. The main idea of ACO is to model a problem as the search for a minimum cost path in a graph. Problem under study is be transformed into the weighted construction graph [14]. The artificial ants incrementally build solutions by moving on the graph to find shortest path. Shortest paths are found as the emergent result of the global cooperation among ants in the colony. The behavior of artificial ants is inspired from real ants:

1. Real ants are blind and communicate with each other by laying a substance named pheromone on the path. This path is called pheromone trails.
2. An isolated ant when encountered with this pheromone trail, it decides to follow the same path and this pheromone become denser as, this ant also lay pheromone on path.

Artificial ants have some extra features as compare to real ants. As, problem firstly is converted into a graph, then ants are initialized here, ants moves node to node. Artificial ants lay pheromone on the graph edges and choose their path with respect to probabilities that depend on pheromone trails. Pheromone trails are updated in following two ways [2, 14]:

1. Firstly, when ants construct a tour they locally change the amount of pheromone on the visited edges by a local updating role.
2. Secondly, after all the ants have built their individual tours, a global updating rule is applied to modify the pheromone level on the edges that belong to the best ant tour found so far.

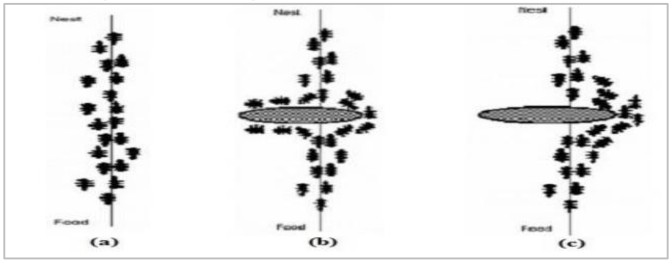

Fig.6: Ants finding the shortest route [2].

Figure 6. Illustrates the basic idea of a real ant system. Figure (a) it can be seen that ants move in a straight line to the food. Figure (b) illustrates the situation soon after an obstacle is inserted between the nest and the food. To avoid the obstacle, different ants randomly choose different path i.e. left or right. Ants that choose to turn left will reach the food sooner, and the ants that prefer to go to right side will take long time. Pheromone accumulates faster in the left side. i.e. shorter path around the obstacle. Since ants follow trails with larger amounts of pheromone, at the end all the ants conjoin to the shorter path around the obstacle.

ACO was first introduced by Marco Dorigo in 1990's. Initially it was referred as ant system. Ant System was originally set of three algorithms. a) Ant Cycle, b) Ant Density,(c) Ant Quantity[12]. In Ant Density and Ant Quantity, the ants updated the pheromone directly after a move from one city to another. In Ant Cycle, the ants updated pheromone when they constructed the tours and deposit the amount of pheromone by each ant was set to a function of the tour quality

because ant cycle performed better than other two variants it was later called simply Ant System. The major merit of AS, whose computational results were promising but not competitive with other more established approaches, was to stimulate a number of researchers to develop extensions and improvements of its basic ideas so as to produce better performing, and often state-of-the-art, algorithm [14, 15].

Later on there comes different extensions of Ant system. Some of which are Elitist ant system, Max-Min ant system (MMAS), Rank-based ant system. In Elitist ant system on every iteration the global best solution deposits pheromone, along with all the other ants. In Max-Min ant system Maximum (τmax) pheromone amount and Minimum (τmin) pheromone amount is added. Only global best or iteration best tour deposited pheromone. In Rank-based ant system all the solutions are ranked according to their length [16, 24].

2.1 Ant Colony Optimization Metaheuristic: A metaheuristic is a general algorithmic which can be used in different optimization problems doing only few modifications according to the problem. The main idea in ACO is to model the problem to be solved into a weighted graph, called construction graph. And then find the optimal path using ants.

Algorithm: Basic flow of ACO
1. Represent the solution space by a construction graph.
2. Set ACO parameters and initialize pheromone trails
3. Generate ant solutions from each ant's walk on the construction graph moderated by pheromone trails.
4. Update pheromone intensities.
5. Go to step 3, and repeat until termination conditions are met.

2.2 Double bridge experiment: In double bridge experiment Deneubourg et al. investigated the pheromone laying and following behavior of ants. The colony of ants was connected to a food source by a bridge having two branches. The experiment was conducted in two parts. In one part both bridges were of same length, in another one bridge length was twice as compare to another one [15]. The ants can reach the food source and get back to the nest using any of the two branches. The goal of the experiment is to observe the resulting behavior of the colony.

I. Both branches having equal length: In the first experiment the bridge had two branches of equal length as shown in figure 7.Initially ants' random chose to follow branch. At the end all the ants used the same branch. When a trial starts there is no pheromone on the two branches. Hence, the ants do not have a preference and they select with the same probability any of the branches [15]. After randomly moving few more ants select one branch over another, thus pheromone becomes denser on that branch and at the end all ants came at one branch.

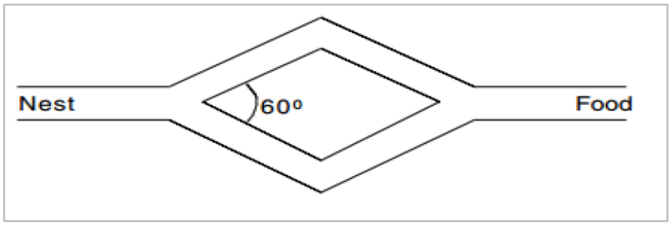

Fig.7: Double bridge experiment with equal length [15]

One branch twice as that of another branch: In the second experiment, one branch was twice as long as another one as shown in figure 8. In this case, all the ants start randomly [15]. It takes less time to come back to colony by following short branch. So, all ants end up at short branch.

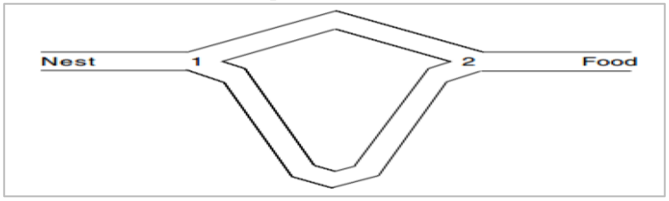

Fig.8: Double bridge experiment with equal length [15]

2..3Ant Colony Optimization for Digital Image feature selection : Feature selection is a very important task in image processing. It can affect performance of system. Feature selection or feature extraction using Ant Colony Optimization can obtain higher processing speed as well as better classification accuracy using a smaller feature set than other existing methods [5]. In ACO base feature extraction ants needs to traverse a complete graph. Feature set is very small yet accurate, thus it consumes less time and space.

Algorithm for ACO based feature selection is as following [5]:

```
Input: DG: The directed graph;
Ʈ: The initial pheromone matrix;
Output: Sbest: The solution of the feature selection
Begin
1. set the initial values of parameters;
2. While not termination condition do
3. Starting from v0, the m ants traverse on the directed graph according to the probability formula one ach node .After all the m ants reach the node vn, m subsets of features are formed;
4. Evaluate the fitness of the m feature subsets by classifying the training image sets;
5. Update the pheromone and heuristic information on each arc;
6. Select the solution with the highest fitness value found so far as Sbest;
7. End While;
8. Output the result;
End
```

III. 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. Xiong, Chao 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 shows 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 colors of the object. In this work vectors of the three features are combined and then feed into the ANN classifier. 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 extrema 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 neighbour 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.

IV. THE PROPOSED METHOD

A new model has been proposed the following steps:

A. *Proposed steps:* 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. Input the image.
2. Pre-processing of image to remove the noise from the image.
3. Generate the non-overlapping blocks.
4. Store these blocks into a metrics.
5. Initialize the Grey wolf Optimization algorithm.
6. Optimize parameters are given by GWO
7. If objective is optimized then converge otherwise artificial bee colony optimization algorithm is initialized and gives converged output.
8. Check the convergence given by ABC and then classification and detection is started.
9. Calculate the accuracy, precision and recall.

B. *Proposed methodology: Flowchart*

This section includes the proposed methodology based on the steps proposed in the earlier section.

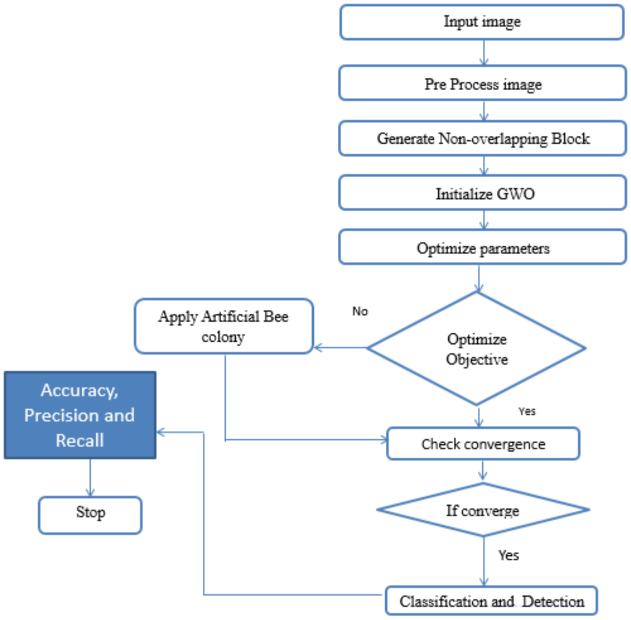

Fig.9 Proposed Flowchart

C. *Algorithm Used*

Grey Wolf Optimizer (GWO): The latest bio-inspired algorithm is the grey wolf optimization algorithm. This algorithm's main concept is simulating the behavior of grey wolf living in a pack. They have a serious hierarchy of social dominance. Alpha is known as the level leaders and is responsible for decision making in the pack. The wolf pack persistence is based on the decision of alpha. Beta is known as the second level subordinate wolves. The beta operation is for help in making the decision for alpha or other activities. Delta is known as the third level subordinate wolves. This category member consists of elders, scouts, hunters, caretakers, and sentinels. For region boundary observation and in any danger case, scouts are liable for the warning. The protection and pack's safety guarantee is given by sentinels. The expertise wolves are the elders, denoted as alpha or beta. Alphas and betas are helped by hunters while prey hunting and caring for the ill, weak, and wounded wolves by caretakers and providing food for a pack. Omega is the lowest level. All dominant wolves with omega wolves have to comply. Grey wolves have the ability of memorizing the prey position and encircling them. The alpha as a leader performs in the hunt. For simulating the grey wolves hunting behavior in the mathematical model, assuming the alpha (α) is the best solution. The second optimal solution is beta (β) and the third optimal solution is delta (δ). Omega (ω) is assumed to be the candidate solutions. Alpha, beta, and delta guide the hunting while position should be updated by the omega wolves by these three best solutions consideration.

Encircling prey: Prey encircled by the grey wolves during their hunt. Encircling behavior in the mathematical model, below equations is utilized.

$$\vec{A}(T+1) = \overrightarrow{A_P}(T) - \vec{X}.\vec{Z}$$

$$\vec{Z} = \left|\vec{Y}.\overrightarrow{A_P}(T) - \vec{A}(T)\right|$$

Where

T←iterative number

$\vec{A}$←grey wolf position

$\overrightarrow{A_P}$←prey position

$$\vec{X} = 2x.\vec{r_1} - x$$

$$\vec{Y} = 2\vec{r_2}$$

Where

$\vec{r_1}$and $\vec{r_2}$←random vector range[0,1]

The x value decreased from 2 to 0 over the iteration course.

$\vec{Y}$← Random value with range [0, 1] and is used for providing random weights for defining prey attractiveness.

Hunting: For grey wolves hunting behavior simulation, assuming α, β, and δ have better knowledge about possible prey location. The three best solutions firstly and ω (other search agents) are forced for their position update in accordance to their best search agents position. Updating the wolves' positions as follows:

MaxI←total number of iteration

$$\vec{A}(T+1) = \frac{\overrightarrow{A_1}+\overrightarrow{A_2}+\overrightarrow{A_3}}{3}$$

(1)

Where $\overrightarrow{A_1},\ \overrightarrow{A_2}, and\ \overrightarrow{A_3}$ are determined,

$$\overrightarrow{A_1} = \left|\overrightarrow{A_\alpha} - \overrightarrow{X_1}.Z_\alpha\right|$$

$$\overrightarrow{A_2} = \left|\overrightarrow{A_\beta} - \overrightarrow{X_2}.Z_\beta\right|$$

$$\overrightarrow{A_3} = \left|\overrightarrow{A_\delta} - \overrightarrow{X_3}.Z_\delta\right|$$

Where $\overrightarrow{A_\alpha},\ \overrightarrow{A_\beta}, and\ \overrightarrow{A_\delta}$← first three best solution at a given iterative T

Z_α, Z_β, and Z_ω are determined,

$$\overrightarrow{Z_\alpha} \leftarrow \left|\overrightarrow{Y_1}.\overrightarrow{A_\alpha} - \vec{A}\right|$$

$$\overrightarrow{Z_\beta} \leftarrow \left|\overrightarrow{Y_2}.\overrightarrow{A_\beta} - \vec{A}\right|$$

$$\overrightarrow{Z_\delta} \leftarrow \left|\overrightarrow{Y_3}.\overrightarrow{A_\delta} - \vec{A}\right|$$

The parameter x updating is the final process. The parameter x exploitation and exploration is updated linearly for ranging [2, 0] in every iteration.

$$x = 2 - t\frac{2}{maxI}$$

Where

T←iterative number

```
Algorithm:  Hybrid GWO_ABC
    1.   Initialize GWO $A_i$(i=1, 2, …n)
Initialize x, X, and Y
Step 1 :Calculate fitness function for every search agent
$A_\alpha$←best search agent
$A_\beta$← second beat search agent
$A_\delta$← Third best search agent
    2.   While (T<Max iterations)
  For ($X_i$ in every pack)
        Update current position of wolf by eq. (1)
        Update x, X and Y
        Calculate the fitness function for all search agents
        Update $A_\alpha$, $A_\beta$, and $A_\omega$
  End for
        For best pack insert migration ($m_i$)
        Evaluate fitness function for new individuals selection of best pack
        New random individuals for migration
End if
End while
3. Input this into Ant bee colony algorithm.
 Initialize ABC Parameters, these parameters are in the forms of bees.
Initialization Phase
The initial food sources are randomly produced  by the equation
        $x_m = l_i + rand(0,1) * (u_i - l_i)$………………………..…………(i)
Where $u_i$ and $l_i$  are the upper bond and lower bond of the solution space of objective function, rand (0, 1) is a random number with in the range [0, 1].
Employed Bee Phase
The neighbor food source $v_{mi}$is determined and calculated by the following equation.
        $v_{mi} = x_{mi} + \Phi_{mi}(x_{mi} - x_{ki}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.(ii)$
Where i is a randomly selected parameter index, $x_k$ is a randomly selected food source, $\phi_{mi}$ is a random number within the range [-1, 1]. The fitness is calculated by the following formula (3), after that a greedy selection is applied between $x_m\ and\ v_m$.
    $fit_m(x_m) = \frac{1}{1+f_m(x_m)}, f_m(x_m) > 0$  and  $fit_m(x_m) = 1 + |f_m(x_m)|\ , f_m(x_m) < 0 \ldots\ldots..(iii)$
Where, $f_m, (x_m)$is the objective function value of$x_m$.
Onlooker Bee Phase
 The quantity of food source is evaluated by its profitability and the profitability of all food sources.
4. Calculate the accuracy, precision and recall.
```

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:

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

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., α 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:

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

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:

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

Where

Q←constant that is predefined,

L_k← length of the tour.

ALGORITHM ACO

Step 1: Initializing ants, where for each ant$_n$, n=1,2,3……..N.

Step 2: In ant$_n$, each variable $\mathbf{x_n^d}$, d=1,2,3…….D.

Step 3: Updating pheromones by choosing $\mathbf{\mu_i^d}$ from the pheromone table with probability in eq. (1), where i∈{1,2,3……K}.

Step 4: If minimum error is obtained, then it has higher probability.

Step 5: Generating a standard deviation $\mathbf{\sigma_i^d}$, if rv ≤ x_1 by eq (2) with the use of uniform distribution U (0,1), where rv is the random value lies between x_1, the predefined threshold 0 and 1.

Step 6: Generating a new value for variable $\mathbf{x_n^d}$: if rv ≤ x_2, by normal distribution N ($\mathbf{\mu_i^d}$, $\mathbf{\sigma_i^d}$).

V. RESULTS

5.1 Performance Metrics: The following quantitative metrics are used to evaluate the performance.

(a) 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.

Acc. = 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

(b) 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)

(c) 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)

(d) True positive rate: TPR refers to the positive samples proportion which predicts correctly as shown below:

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

(e) 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.

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

4.2 Detection

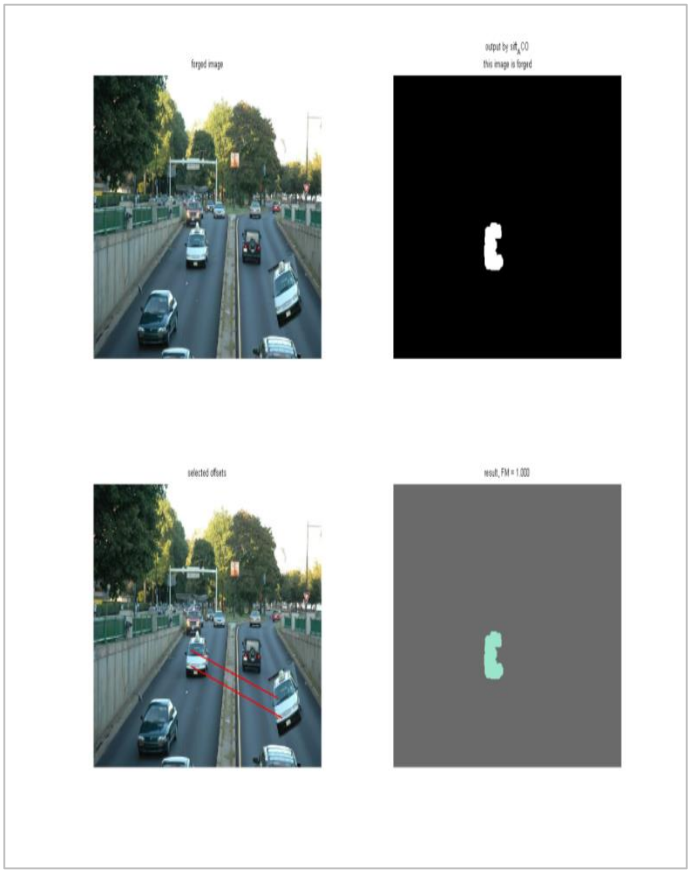

Fig.10:Analysis of SIFT GWO_ABC features Detection

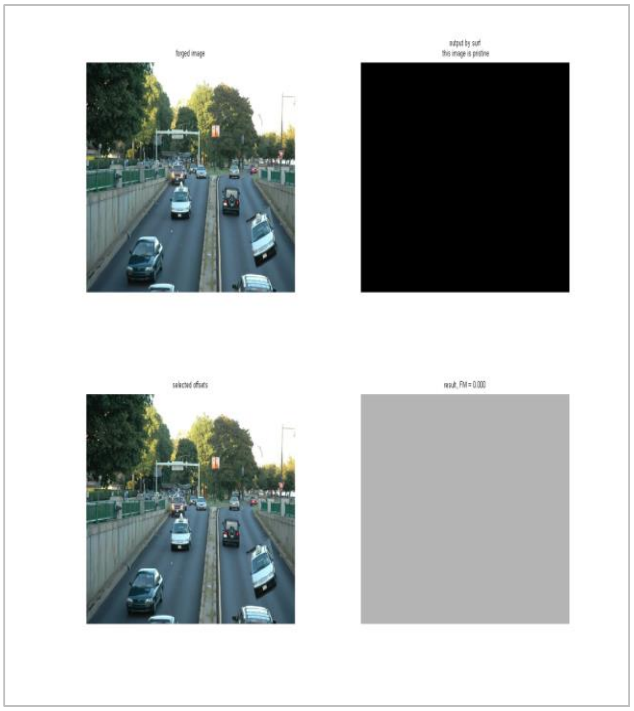

Fig.11:Analysis of SIFT ACO features Detection

Above given fig.10 and fig.11 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 features detect.

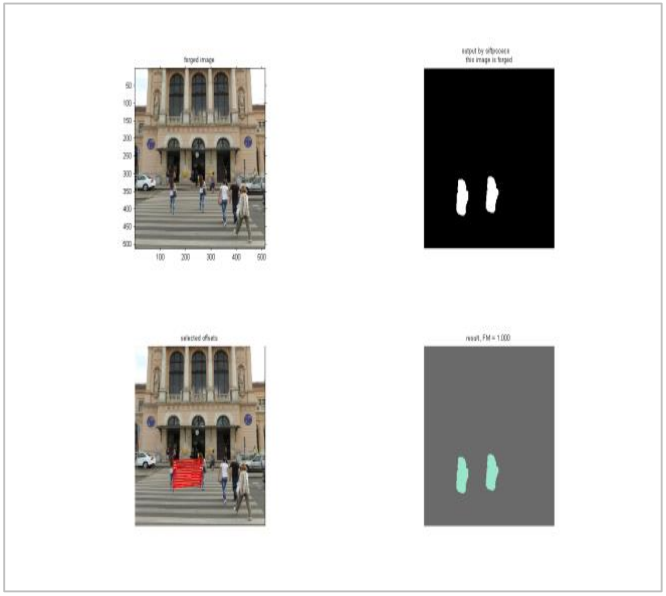

Fig. 12:Sift GWO_ABC

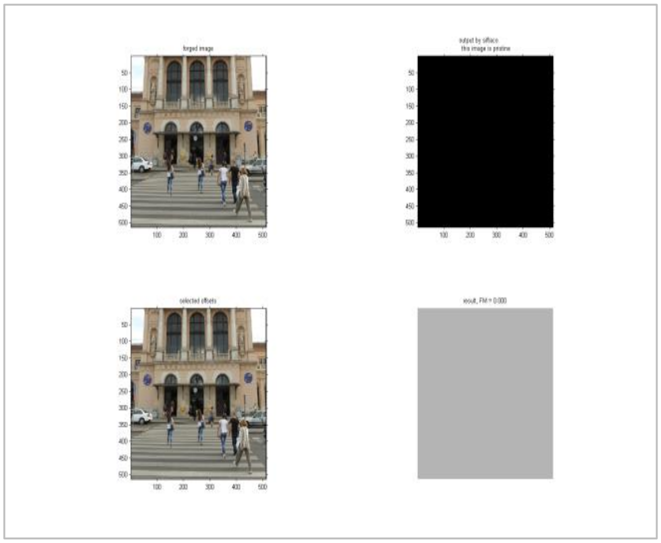

Fig.13:SIFT-ACO

Table.1:Precision of different classifier

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

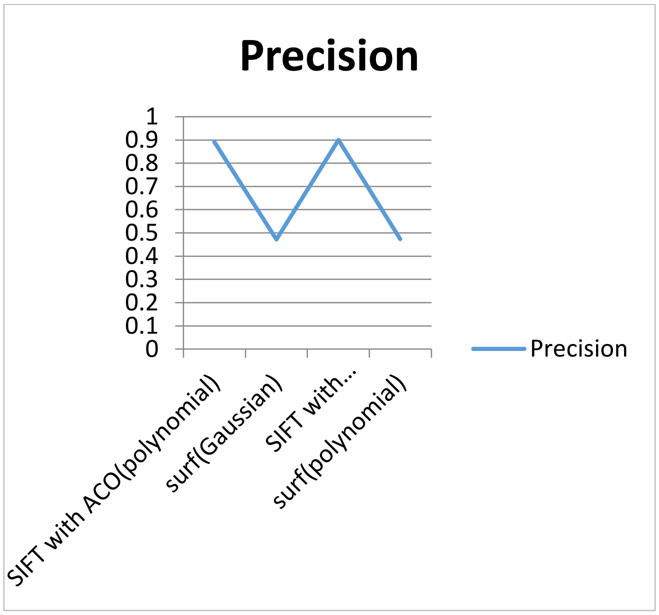

Fig.14:Precision of classifiers

Fig.14 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 show the maximum precision is on SIFT with GWO_ABC (Gaussian) classifier and minimum is on surf (Gaussian).

Table.2:Accuracy Graphs of 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

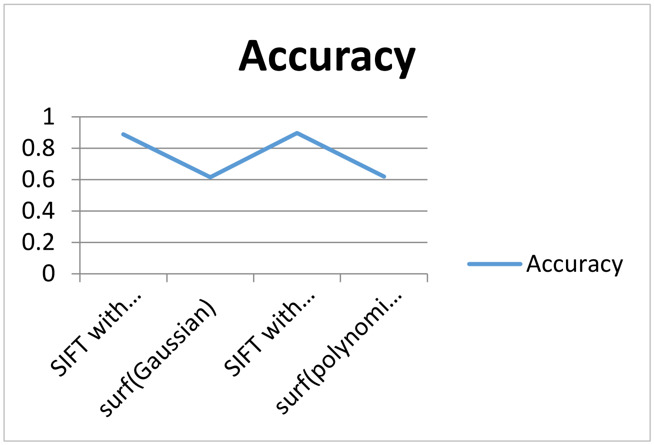

Fig.15 :Accuracy of classifiers

Fig.15 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.3: Recall of 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

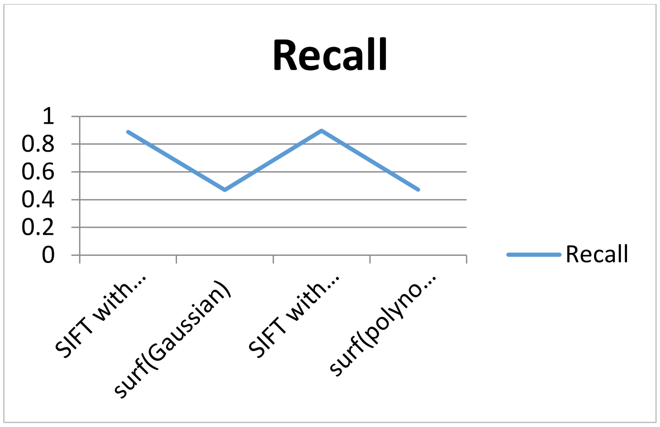

Fig.16: Recall of classifiers

Fig.16 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 4.4 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
SIFT with GWO_ABC (Gaussian)	0.9	0.8979	0.8963
Surf (polynomial)	0.4737	0.6193	0.4726

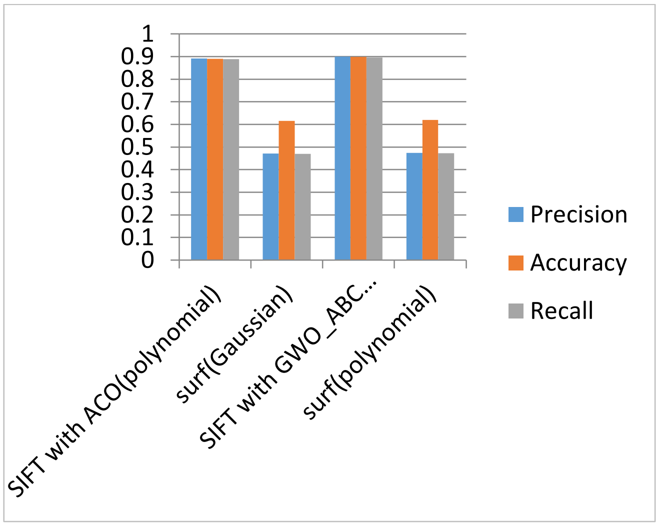

Fig.17 :Comparison of Parameters

Fig.17 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.

VI. CONCLUSION

In proposed versatile over division calculation sections the host picture into no overlapping and sporadic blocks adaptively. Then, the element focuses are removed from each block as block elements, and the block components are coordinated with each other to find the named highlight focuses; this technique can around show the presumed forgery districts. In past few years, Copy-move forgery is a very common way to tamper an image. Many researchers have proposed various schemes to detect the tampered images. Sometimes the copied regions are rotated or flipped before being pasted. In this paper. In this paper propose Detection and classification method by machine learning and optimization method. In our experiment detection and classification with sift ACO and SVM Gaussian and polynomial kernel. SIFT with ACO with polynomial kernel and SIFT with GWO_ABC with polynomial Kernel show significance high accuracy, precision and recall.

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, Honglei Guo, 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, Mohd Shafry Mohd 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*.

[14]. Bi, X., Pun, C. M., & Yuan, X. C. (2016). Multi-level dense descriptor and hierarchical feature matching for copy–move forgery detection. *Information Sciences*, *345*, 226-242.

[15]. Wen, B., Zhu, Y., Subramanian, R., Ng, T. T., Shen, X., & Winkler, S. (2016, September). COVERAGE—A novel database for copy-move forgery detection. In *Image Processing (ICIP), 2016 IEEE International Conference on* (pp. 161-165). IEEE.