Novel Approach of Copy move forgery detection and classification by Ant Bee Colony and swarm intelligence

Kanika Sood[1], Dr. Rajiv Dahiya [2]
[1, 2]ECE, PCET
(Sood.kanika.kannu@gmail.com[1] ,raj8878@gmail.com[2])

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 artificial 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—*Artificial Ant Colony System, Ant Colony Optimization, Particle Swarm Optimization, Color Coherence Vector.*

I. INTRODUCTION

A. Copy-Move Forgery

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. 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 [1, 4]. 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 [3]. It has begun such an era where seeing is no longer believing. 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. 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.

B. Digital Image forgery

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]. 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.

C. 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) *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. 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.
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 [11].
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.
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.
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, 22]. Copy Move involves copying regions of the original image and pasting into other areas.

D. 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 Source Image [3]

Fig.2 :Output Forged Images [3]

E. 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 are 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:

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

F. 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]. In fig.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. 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 [9].

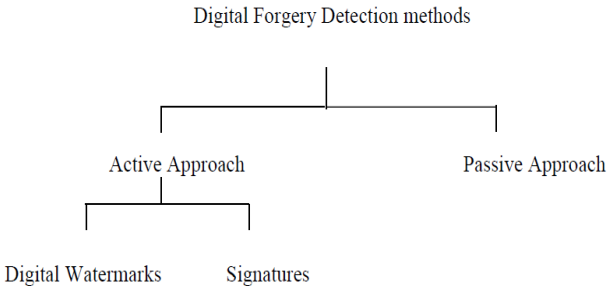


Fig.3 :Digital Forgery detection Methods [10]

1.6.1 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 [2]. 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.

1.6.2 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.

G. 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 fig.4.

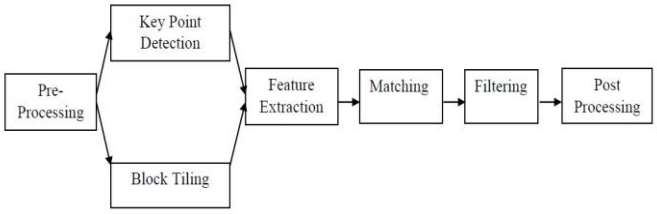


Fig.4 :Common processing pipeline for Copy Move Forgery Detection [21]

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.

1.7.1 Key Point Based Copy-Move Forgery Detection: 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. In case of 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.

1.7.2 Block 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 [1]. 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.

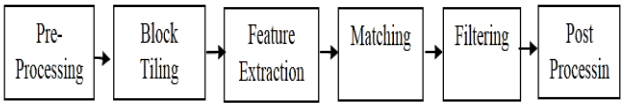


Fig.5: Common processing pipeline for Copy Move Forgery Detection [21].

Following Steps are performed for Copy Move forgery detection:

- *Block Tiling:* In this step image is divided into n by n non-overlapping blocks.
- *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].
  - 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].
  - 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].
  - 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 [10].

1.7.3 Selection of CMFD Method: While selecting the CMFD algorithm the following criteria should be considered: The algorithm should allow approximate match for small segments. It should be able to withstand all kind of attacks and be sensitive to low contrast image areas. Also, the results of producing false positive should be minimal. The detected forged areas or segments should have some sort of connections rather than a collection of small patches. The selected detection algorithm should be robust enough also. The chances for occurrences of the various attacks within a copy move forgery is very low [6]. This is due to the reason that source and target are from same image, thus the properties like colour, temperature, illumination conditions and noises are not affected. While searching for forgery areas, any of the following two approaches can be used.

1.7.3.1 Exhaustive Search Method & Autocorrelation

Exhaust search method is that first the input image is eroded followed by dilation. This approach is very much effective but computational cost is very high. Whereas in autocorrelation a strong mathematical support is used with the Fourier transform. Both the original and the tampered images will introduce some peaks. By checking these peaks, it is possible to and the cloned areas. A high pass filter is used along with this autocorrelation. Any kind of detection system should be tested using the image in both image level and pixel level [7]. From image level it is possible to conclude that whether the chosen algorithm can or can't detect the cloned regions. And with the pixel level testing the level of accuracy of the tampered regions is identified.

H. Ant Colony Optimization

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:

(a) Real ants are blind and communicate with each other by laying a substance named pheromone on the path. This path is called pheromone trails.

(b) 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 laid 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]:

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.

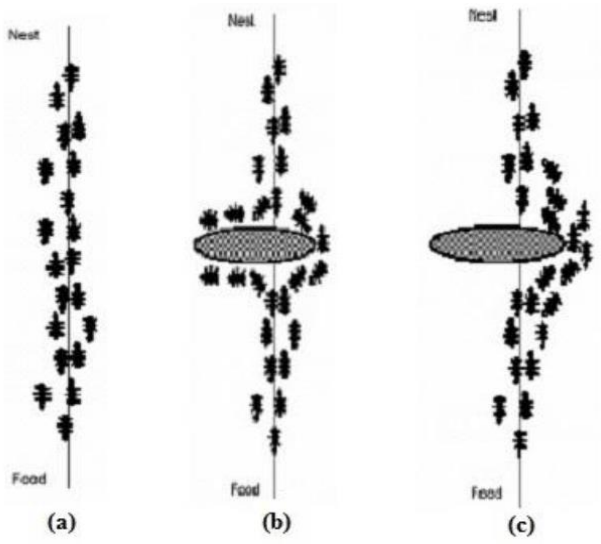


Fig.6: Ants finding the shortest route [2].

Fig.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 [13]. 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]. 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 [12].

1.8.1 Ant Colony Optimization Meta-Heuristic: A meta-heuristic 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.

1.8.2 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. The ants can reach the food source and get back to the nest using any of the two branches [6, 8]. The goal of the experiment is to observe the resulting behavior of the colony.

a) Both branches having equal length: In the first experiment the bridge had two branches of equal length as shown in fig.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. 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.

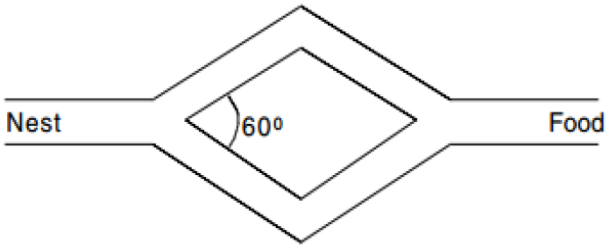


Fig.7: Double bridge experiment with equal length [14]

b) 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 [24]. It takes less time to come

back to colony by following short branch. So, all ants end up at short branch.

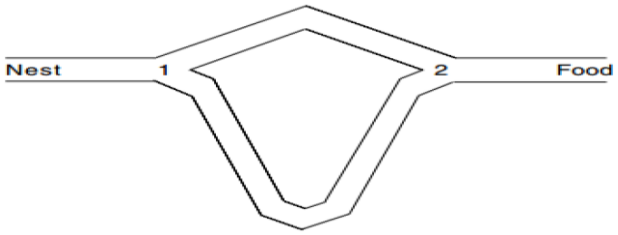


Fig.8: Double bridge experiment with unequal length [14]

1.8.3 Ant 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;

Ƭ: 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

II. RELATED WORK

Chi-Man Pun, et al. [1] In this paper authors proposed a novel copy-move forgery detection scheme using adaptive over segmentation and feature point matching. The proposed scheme integrates both block-based and Keypoint-based forgery detection methods. First, the proposed adaptive over segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labelled feature points; this procedure can approximately indicate the suspected forgery regions. The experimental results indicate that the proposed copy-move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy-move forgery detection methods.E. Ardizzone et al. [2] et al. In this paper authors presented a very novel hybrid approach, which compares triangles rather than comparing blocks or single points. Interest points are extracted from the image and objects are modelled as a set of connected triangles using these points. Triangles are matched according to their shapes, their content, and the local feature vectors extracted onto the vertices of the triangles. Proposed method is designed to be robust to geometric transformations. Results were compared with a block matching method and a point-based method.

Alkawaz, M. H., et al. [3] this paper proposed the forgery detection method using discrete cosine transform. DCT is used to identify the tampered region from the image. In this work the image is converted first RGB to grey scale and then divide the image into block. Zig-Zag scanning is used for every block to calculate the feature vector. These feature vectors are sot by using lexicographic sort. Duplicated block are identified by using Euclidean distance method. The performance evaluation of the proposed method is done on the basis of parameters like storage, accuracy and threshold. Bi, X., Pun, et al. [4] in this paper, the author proposed Multi-level Dense Descriptor method for extraction and feature matching method for forgery detection in the images. This method detects the feature descriptor using multiple levels. Dense descriptor extracts by using color descriptor and Invariant moment descriptor. This method detects the similar features on the basis of textures. Morphological operations are applied to detect the forgery. This method performs better than existing methods and approaches in duplicate region detection. Bi, X., Pun, et al. [5] in this paper, the author proposed Multi-level Dense Descriptor method for extraction and feature matching method for forgery detection in the images. This method detects the feature descriptor using multiple levels. Dense descriptor extracts by using color descriptor and Invariant moment descriptor. This method detects the similar features on the basis of textures. Morphological operations are applied to detect the forgery. This method performs better than existing methods and approaches in duplicate region detection. Rao, Y., & Ni, et al. [6] Convolution neural network is used to detect the forgery in the images. In this method weights are assigned at first layer of network and high pass filter is used to calculate residual maps. Dense features are extracted by using CNN as patch descriptor on images. In SVM classification discriminative features are used. This method performs better than existing

methods and approaches in duplicate region detection. Ferreira, A., et al [7] in this paper, the author proposed Behavior knowledge space-based fusion for copy-move forgery detection. This technique is based on the multi-directionality of data to the final output in machine learning decision making fashion. This method performs better than existing methods and approaches in duplicate region detection. Dixit, A., et al. [8] 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. Agarwal, V., et al [9] 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. M. Buvana Ranjani et.al. [10] Proposed a method which is based on the DCT and IDCT transform techniques. This method reduces the computational complexity which related to the cost and time. The DCT method works on the rows and columns reduction and transforms them into the blocks. The result of the simulation shows that it provides the effective result and improves the complexity. **Shi** Wenchang [11] in this paper authors proposed a method to implement Copy Move Forgery Detection with Particle Swarm Optimization. CMFD-PSO integrates the Particle Swarm Optimization (PSO) algorithm into the SIFT-based framework. It utilizes the PSO algorithm to generate customized parameter values for images, which are used for CMF detection under the SIFT-based framework. Experimental results show that CMFD-PSO has good performance. Yong-Dal Shin, et al [12] in this paper, author proposed fast exploration method of copy-move forgery image. A new simple search algorithm using a half block size for copy-moved forgery image detection is proposed. Proposed algorithm reduced computational complexity more than conventional algorithms. In this author didn't use 8x8 pixel block exhaustive search method and frequency algorithm to reduce computational complexity.

Devanshi Chauhana, et al. [13] one of the problems in image forensics is to check the authenticity of image. This can be very important task when images are used as an evidence which cause change in judgment like, for example in a court of law. In this author has done a survey on different Key point based copy-move forgery detection methods with different parameters.

III. THE PROPOSED METHOD

A. Proposed Methodology

In this design methodology firstly, image is converted into overlapping blocks after converting into grey scale, then features are extracted using Grey wolf Optimization, then matching will be performed using Artificial Bee colony 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 grayscale image into overlapping blocks.
4) Store these blocks into a metrics.
5) Extract feature vectors using Grey wolf Optimization.
6) Match similar feature vectors using Artificial Bee colony.
7) Initialize ants.
8) Evaluate results and update Wolf values.
9) Check if exit criteria met.
10) If yes give final detected forged regions, else initialize new BEES.

B. Proposed methodology: Flowchart

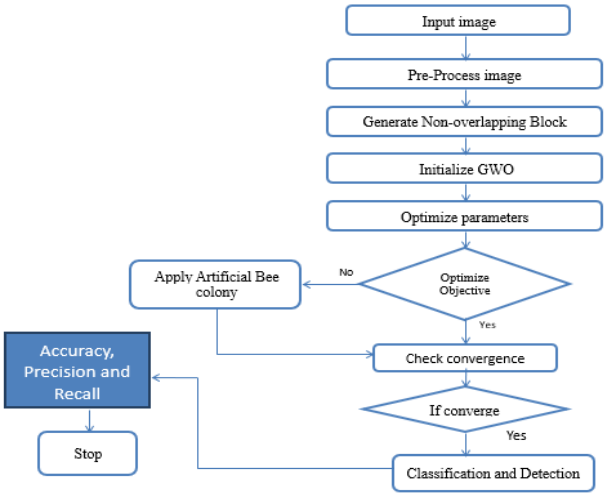


Fig.9 :Proposed Flowchart

C. Description of Algorithm used

The following is the detail of the different algorithms used in the present work.

(a) 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 considerations.

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

$$\vec{X} = 2x.\overrightarrow{r_1} - x$$
$$\vec{Y} = 2\overrightarrow{r_2}$$

Where
$\overrightarrow{r_1}$and $\overrightarrow{r_2}$←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:

$$\vec{A}(T+1) = \frac{\overrightarrow{A_1}+\overrightarrow{A_2}+\overrightarrow{A_3}}{3}$$
(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 are updated linearly for ranging [2,0] in every iteration.

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

Where
T←iterative number
MaxI←total number of iterations

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_α←best search agent A_β← second beat search agent A_δ← 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_α, A_β, and A_ω
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

$$x_m = l_i + rand(0,1) * (u_i - l_i) \ldots\ldots\ldots (i)$$

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.

$$v_{mi} = x_{mi} + \Phi_{mi}(x_{mi} - x_{ki}) \ldots\ldots\ldots (ii)$$

Where i is a randomly selected parameter index, x_k is a randomly selected food source, ϕ_{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.

$$fit_m(x_m) = \frac{1}{1+f_m(x_m)}, f_m(x_m) > 0 \text{ and } fit_m(x_m) = 1 + |f_m(x_m)|, f_m(x_m) < 0 \ldots\ldots (iii)$$

Where, $f_m, (x_m)$is the objective function value ofx_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.

(b) Ant Colony Optimization (ACO): 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 travelling 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:

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

Where

$\eta_{xy} \leftarrow$priority heuristic information,

$\tau_{xy} \leftarrow$ 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:

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

Where

$\rho \leftarrow$ Pheromones rate of trail evaporation,

N$\leftarrow$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:

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

Where

Q$\leftarrow$constant that is predefined,

$L_k \leftarrow$ 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 x_n^d, d=1,2,3……. D.
Step 3: Updating pheromones by choosing μ_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 σ_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 x_n^d: if rv ≤ x_2, by normal distribution N (μ_i^d, σ_i^d).

(c) SVM with Normal: Utilizing Support Vector Machine (SVM) algorithms for classification. Classification can be viewed as the separating classes task in feature space.

Step1: Given training data (x_i, y_i) for i=1…...N,
with $x_i \in R^7$ and $y_i \in$ {0 to 6}
$f(x_i)$ = 00111*{>0 y_i=+1,
<0 y_i= -1}

Step 2: make model
$f(x)= (w^t x +b)$ *00111
Initialize w=0

Step 3: Check the data points {x_i, y_i}
if x_i misclassified them
ww +α Sign ($f(x_i)$) x_i
Run Step 3 until data is correctly classified

Step 4: Select best w
W*Normal function

Step 5: Then margin given

$$\frac{w}{\|w\|}(x_+ - x_-) = \frac{w^t(x_+ - x_-)}{\|w\|} = \frac{2}{\|w\|}$$

Step 6: Optimize SVM

$$\max_w \frac{2}{\|w\|}$$

Step 7: Test optimize SVM with Normal model
Step 8: Analysis precision, Recall, Accuracy.

(d) SVM with RBF Kernel: Many learning calculations can just do direct classification, utilizing a straight line to isolate the information focuses. In any case, support vector machines being one of them that can likewise do non-direct classification utilizing a kernel technique.

Nonlinear Classification gives a more modern approach to arrange complex informational indexes that can't undoubtedly be isolated by a straight line. Kernel utilized for Make non-divisible issue distinct and Map information into better representational space.

Step1: Given training data (x_i, y_i) for i=1…...N,
with $x_i \in R^7$ and $y_i \in$ {0 to 6}
$f(x_i)$ = 00111*{>0 y_i=+1,
<0 y_i= -1}

Step 2: make model
$f(x)= (w^t x +b)$ *00111
Initialize w=0

Step 3: Check the data points {x_i, y_i}
if x_i misclassified them
ww +α Sign ($f(x_i)$) x_i
Run Step 3 until data is correctly classified

Step 4: Select best w
W*RBF function

Step 5: Then margin given

$$\frac{w}{\|w\|}(x_+ - x_-) = \frac{w^t(x_+ - x_-)}{\|w\|} = \frac{2}{\|w\|}$$

Step 6: Optimize SVM

$$\max_w \frac{2}{\|w\|}$$

Step 7: Test optimize SVM with RBF model
Step 8: Analysis precision, Recall, Accuracy.

3.5.5 SVM with MLP Kernel

The Multilayer Perception (MLP) is the most popular network architecture in use both for classification and regression. The MLP has one or more hidden layers between the input layer and the output layer.

Step1: Given training data (x_i, y_i) for i=1…...N,
with $x_i \in R^7$ and $y_i \in$ {0 to 6}
$f(x_i)$ = 00111*{>0 y_i=+1,
<0 y_i= -1}

Step 2: make model
$f(x)= (w^t x +b)$ *00111
Initialize w=0

Step 3: Check the data points {x_i, y_i}
if x_i misclassified them
ww +α Sign ($f(x_i)$) x_i
Run Step 3 until data is correctly classified

Step 4: Select best w
W*MLP function

Step 5: Then margin given

$$\frac{w}{\|w\|}(x_+ - x_-) = \frac{w^t(x_+ - x_-)}{\|w\|} = \frac{2}{\|w\|}$$

Step 6: Optimize SVM

$$\max_w \frac{2}{\|w\|}$$

Step 7: Test optimize SVM with MLP model
Step 8: Analysis precision, Recall, Accuracy.

IV. RESULT ANALYSIS

A. 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.

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

B. Detection:

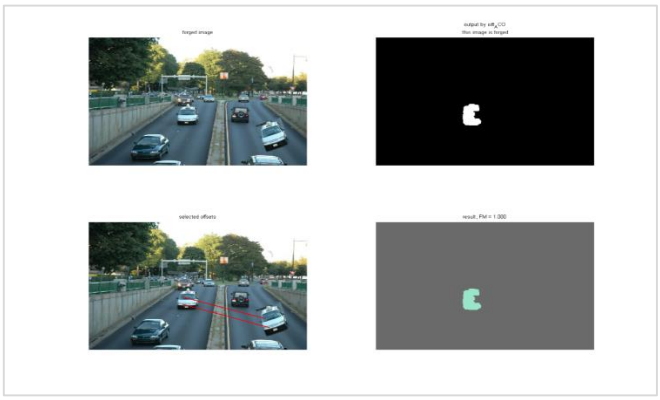


Fig.10: Analysis of SIFT GWO_ABC features Detection

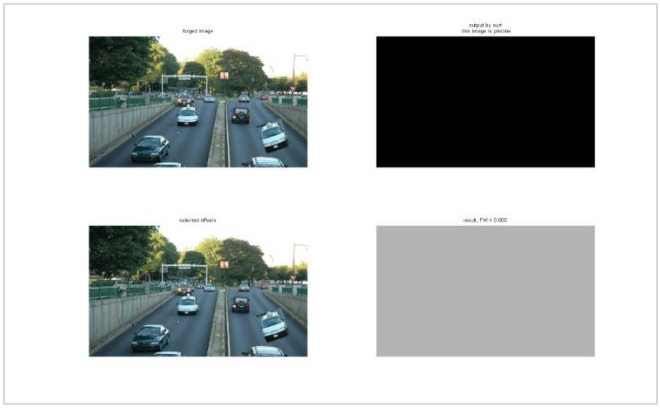


Fig.11: Analysis of SIFT ACO features Detection

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.

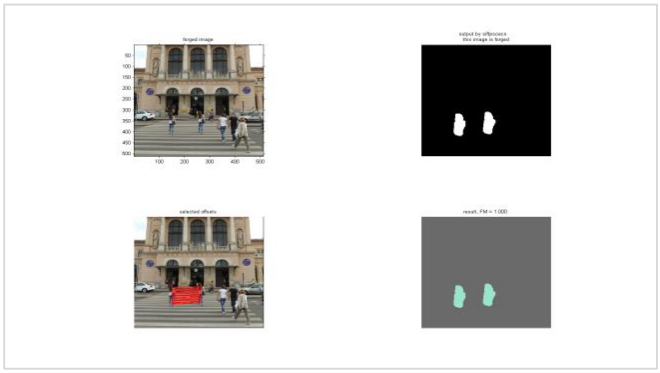


Fig.12: SIFT GWO_ABC

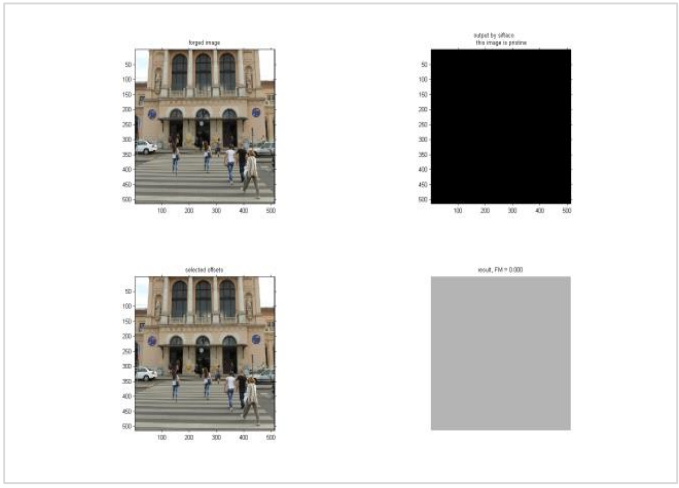


Fig.13: SIFT-ACO

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

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

Table. 4.1: Precision Value for Different Classifier

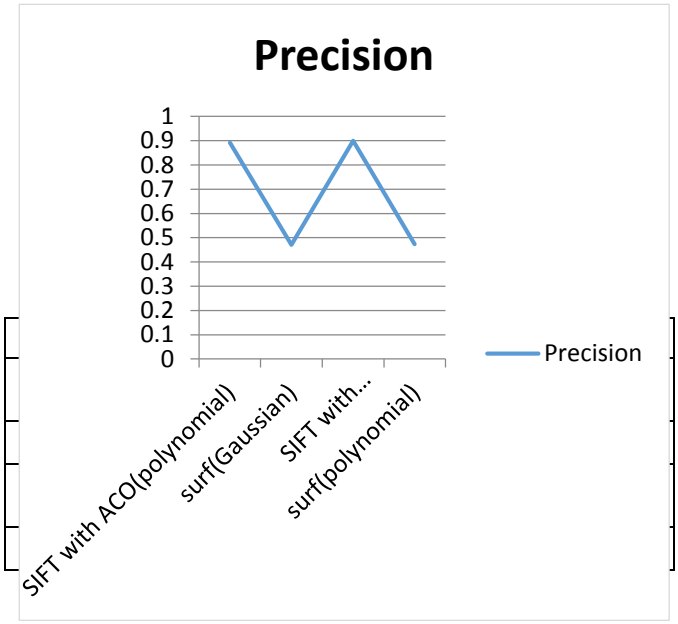


Fig.13: Graph showing the precision for different classifiers

Fig.13 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. 4.2 :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

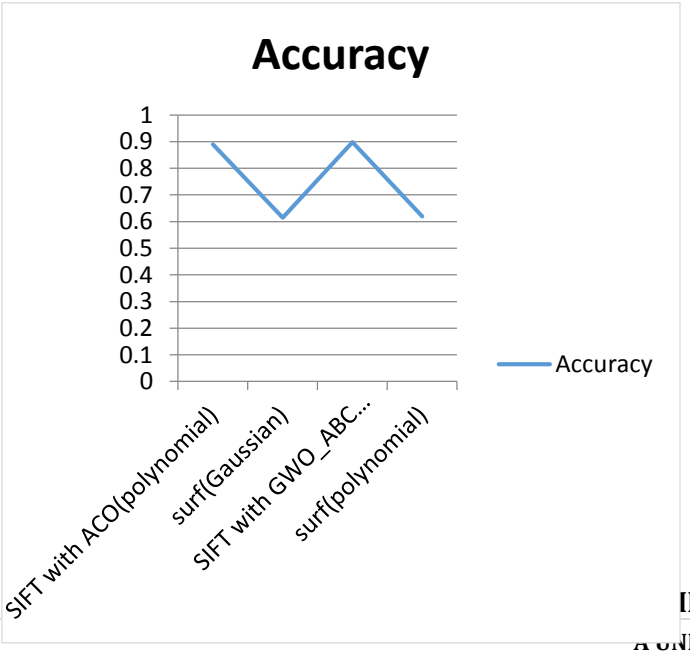


Fig.14: Graph showing the accuracy value for different classifiers

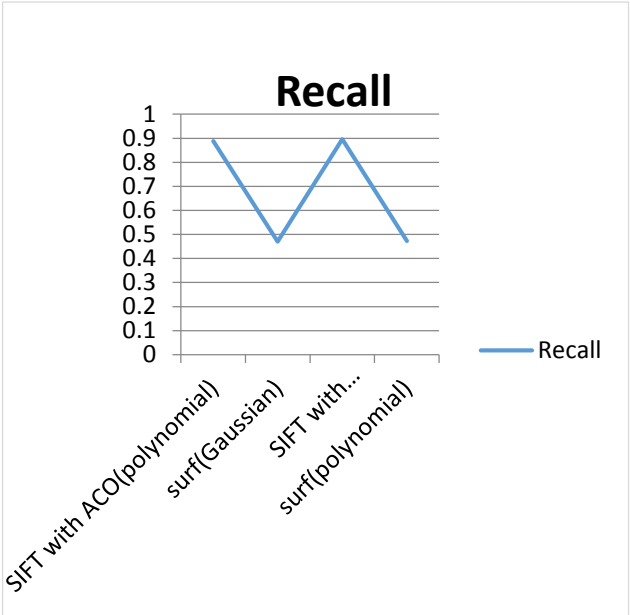
Fig.14 depicts the accuracy of the four classifiers that are SIFT with ACO (polynomial), surf (Gaussian), SIFT with GWO_ABC (Gaussian) and surf (polynomial). SIFT with GWO_ABC (Gaussian) shows the maximum accuracy classifier and minimum is on surf (Gaussian).

Table .4.3: Recall Value for Different Classifier

Fig .15: Graph showing the Recall value for different classifiers

Fig.15: 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

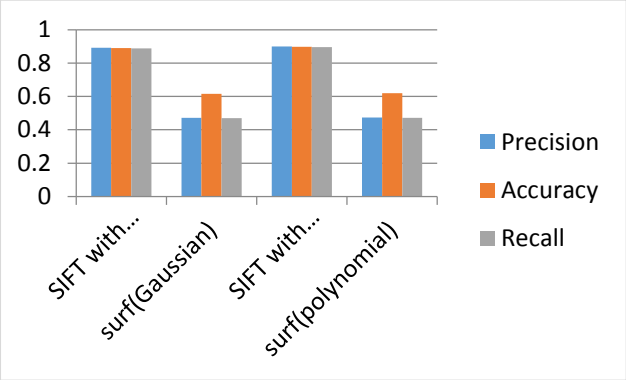


Fig.16: Graph showing the comparison of all the parameters

Fig.16 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.

V. CONCLUSION

In present 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 show the presumed forgery blocks in the images. 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 thesis, detection and classification methods are done by using the machine learning with optimization method. In the present work forgery detection and classification is done by using SIFT with ACO and SIFT GWO_ABC with SVM Gaussian and polynomial kernel but GWO_ABC show significance high accuracy, precision and recall in case of classification.

REFERENCES

[1]. Chi-Man Pun, Xiao-Chen Yuanand Xiu-Li Bi, "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching", IEEE Transactions on Information Forensics and Security, Volume 10 , Issue 8, Aug. 2015, pp. 1705 – 1716.

[2]. E. Ardizzone, A. Bruno, and G. Mazzola" Copy-Move Forgery Detection by Matching Triangles of Keypoints", IEEE Transactions on Information Forensics and Security ,Volume 10 , Issue 10 , Oct. 2015,pp 2084 – 2094.

[3]. Alkawaz, M. H., Sulong, G., Saba, T., & Rehman, A. (2016). Detection of copy-move image forgery based on discrete cosine transform. *Neural Computing and Applications*, 1-10.

[4]. 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.

[5]. 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.

[6]. Rao, Y., & Ni, J. (2016, December). A deep learning approach to detection of splicing and copy-move forgeries in images. In *Information Forensics and Security (WIFS), 2016 IEEE International Workshop on* (pp. 1-6). IEEE.

[7]. Ferreira, A., Felipussi, S. C., Alfaro, C., Fonseca, P., Vargas-Munoz, J. E., dos Santos, J. A., & Rocha, A. (2016). Behavior Knowledge Space-Based Fusion for Copy–Move Forgery Detection. *IEEE Transactions on Image Processing*, *25*(10), 4729-4742.

[8]. Dixit, A., Dixit, R., & Gupta, R. K. (2016). DCT and DWT Based Methods for Detecting Copy-Move Image Forgery: A Review. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, *9*(10), 249-258.

[9]. Agarwal, V., & Mane, V. (2016, September). Reflective SIFT for improving the detection of copy-move image forgery. In *Research in Computational Intelligence and Communication Networks (ICRCICN), 2016 Second International Conference on* (pp. 84-88). IEEE

[10]. M. Buvana Ranjani, R. Poovendran, "Image Duplication Copy Move Forgery Detection Using Discrete Cosine Transforms Method", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 11, Number 4, 2016, pp. 2671-2674.

[11]. Shi Wenchang, Zhao Fei, Qin Bo, Liang Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques", China Communications, Volume 13, Issue, 1, Jan 2016, pp. 139 – 149.

[12]. Yong-Dal Shin, "Fast Exploration of Copy-Move Forgery Image" Advanced Science and Technology Letters, Vol.123 (ISA 2016), pp.1-5.

[13]. Devanshi Chauhana, Dipali Kasatb, Sanjeev Jainc, Vilas Thakared, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image", Elsevier -International Conference on Computational Modeling and Security (CMS 2016), pp. 206 – 212.