IMPROVE COPY MOVE FORGERY IMAGE CLASSIFICATION BY OPTIMIZATION TECHNIQUE

Mehak, Tarun Gulati

Department of ECE, MMEC, MMU, Mullana, Ambala, Haryana, India

ABSTRACT

In our society digital images are a powerful and widely used communication medium. They have an important impact on communication and IT industry. But, in this digital savvy world there is no doubt in saying "seeing is no more believing". So detection is very important challenges for testing in forensic science. In past few years, research goes to detecting and classified for copy move forgery images for forensic requirement. In this paper methodology based on detection and classification by point based and block based features SIFT and SURF is done and uses Ant Colony Optimization in matching and feature selection phases respectively. In case of SIFT and SURF features and proposed SIFT with ACO features, classification is also done by using support vector machine with Gaussian and Polynomial kernel. It is found that SIFT with ACO technique outperforms on another techniques.

Keywords— *ACO, Gaussian Kernel, Polynomial Kernel, SIFT, SURF, SVM.*

I. INTRODUCTION

Due to availability of powerful image processing and editing software the digital images are easy to manipulate. As the image manipulation is said to be a digital state of the art which required the basic need of understanding of properties of digital image and the better visual creativity. One manipulate the image for different reasons either to enjoy the magic of digital works during which amazing photos are created or somehow to produce wrong impression in many genuine world applications. After this modification, image processing software gives the image output which is no longer same as the original image information. So, the consequences regarding security of the images have to be considered seriously. In digital world, there are many detection techniques to detect different kinds of forgery for authentication of images has been proposed currently. Generally, into two major domains the image protection can be divided: (i) active protection in which the original digital image is embedded with watermark from which tampering can be detected through comparison [1]. As in the past times the watermark and digital signatures methods of active domain are used in the images for the detection of tampered regions but for these detection method have to pre-process the data first, which creates difficulty to apply these methods [2]. Also, due to the reason of today's mostly imaging devices like camera do not contain any watermarking and signature module. (ii) Passive protection which relies on the image processing technology but it does not need any digital watermark or signature to detect the forgery. This is usually a great challenge in image processing technique. Here, without adding or assuming any embedding signatures in the image, it deals with analyzing the raw image according to the traces inevitably left

by the tampering process. From the image to make an object "disappear" a part of image is copied and pasted into another part of the same image. For cover-up the "missing" object the textural areas (such as cloudy sky, grass foliage etc.) are ideal because with the background the copied area will likely blend and human eye cannot discern the artefact. In the lossy JPEG format the tampering image is likely saved from which forgery detection become difficult [1]. In this paper, we proposed ACO (Ant Colony Optimization) algorithm to optimize the copy move forgery detection technique. In II section forgery related work is discussed. In III section methodology regarding purposed technique is explained. In the IV section result is presented. In last V section Conclusion is discussed.

II. RELATED WORK

In [3] with features extracted along radius direction an efficient algorithm is proposed which is based on the Fourier-Mellin Transform. A link processing is introduced to reduce computational cost. Furthermore, to cluster distance vectors a vector erosion filter is designed.

In [4] using dyadic wavelet transform (DyWT) a blind copy move image forgery detection method is proposed. For data analysis DyWT is shift invariant and suitable. Firstly, the input image is decomposed into detail (HH1) and approximation (LL1) sub-bands. Then into overlapping blocks, the LL1 and HH1 are calculated and between the blocks the similarity is calculated. From the LL1 sub-band, the similarity is called key idea that should be high, while due to noise inconsistency in the moved block from the HH1 sub-band should be low. Therefore, using the LL1 sub-band pairs of blocks are sorted based on high similarity.

In [5] for copy move forgery detection (CMFD) numerous algorithm have been proposed, for a CMFD new database consists of 260 forged image sets. Two masks, original image and forged image. According to applied manipulation image are grouped in 5 categories: distortion, rotation, scaling combination and translation. Also, such as blurring, noise adding, JPEG compression and color reduction etc. are the post-processing methods are applied at the original images and forged.

In [6] to detect copy-move forgery in digital images effective method is described. To reduce the dimensional representation the technique is works by first applying DWT (Discrete Wavelet Transform) to the input image. Then into overlapping blocks the compressed image is divided. Using Phase correlation these blocks are sorted and copied blocks are identified. On the lowest level image representation the detection is firstly carried out due to DWT usage.

In [7] for detecting copy-move-forgery a new and blind forensics approach is described. To estimate the spatial offset between the pasted region and copied region the phase correlation is computed. By the idea of pixel-matching the copy-move regions can be easily located, according to the spatial offset which shifted the input image and between the images calculate the difference.

In [8] based on the Fourier-Mellin Transform an efficient algorithm is proposed, along with radius direction features are extracted. In the counting bloom filters a link processing is introduced to reduce computational cost. Furthermore, to cluster distance vectors, a vector erosion filter is

designed, in existed copy-move detection algorithm which usually achieved through vector counters.

In [9] with digital images (digital forgeries) the malicious manipulation is detected. The specific digital forgery detection type is the main focus and the copy move forgery attack is referred to the image is copied and pasted to somewhere else in the image. The problem of detecting the copy-move forgery is investigated and a reliable and efficient method is described in this paper.

In [10] from the tampered images to detect the forgery region an algorithm is proposed with more advancement and accuracy. In the form of evaluation parameters of precision, recall and FPR and DAR the results are formed.

In [11] for detecting copy-move forgery a new method is proposed. Into overlapping circular blocks the image is firstly filtered and divided. Using rotation invariant uniform local binary patterns the features of the circular blocks are extracted. By tracking the corresponding blocks the feature vectors are compared and the forged regions can be located.

In [12] for detecting copy-move forgery an efficient expanding block algorithm is proposed. This method is effective in shape and identifying of duplicated region. Moreover, where the region has been manufactured under JPEG compression, slightly lighter with the effect of Gaussian blurring it allows copy-move forgeries to be detected.

III. WORK METHODLOGY

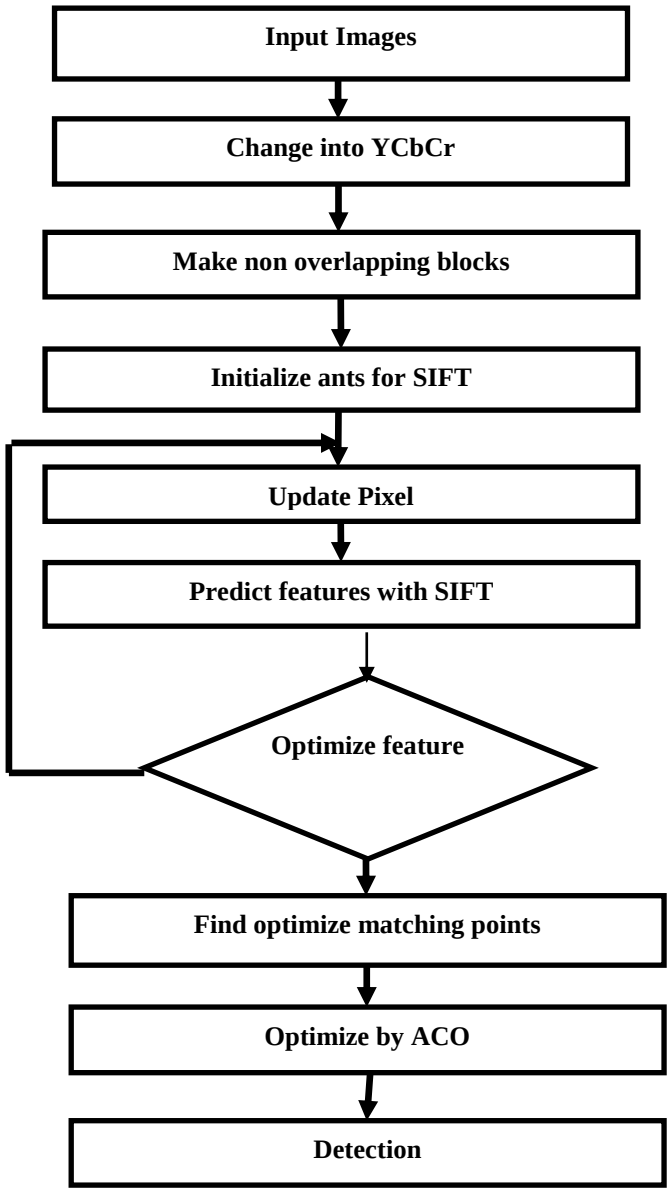

Fig. 3.1: Flow chart of Proposed Methodology

In design methodology as shown in Fig. 3.1firstly image is converted into grey scale and then into overlapping blocks. The feature extracted using Ant Colony Optimization then matching is performed using ACO and locate the forged regions in the original image.

Steps are as following:

1. Take a colored forged image as input.
2. Convert image into Grey Scale.
3. Divide grey scale image into overlapping blocks.
4. Store these blocks into a metrics.
5. Extract feature vectors using Ant colony Optimization.
   5.1. Initialize ants.
   5.2. Evaluate results and update pheromone values.
6. Match similar feature vectors using Ant Colony Optimization.
7. Check if exit criteria met.
8. If yes give final detected forged regions, else initialize new ants.

ALGORITHM:

Step 1: Input copy forgery imaged and not forgery images.

Step 2: Change RGB to YC_bC_r format.

Step 3: Extract the features by Ant colony method

Step 3.1 Initialize the Ants according to pixel.

Step3.2 Extract the feature pixel wise by optimizing difference of non-overlapping blocks.

Step 3.3 Change the pixel difference

$T_{ij} \leftarrow (1\text{-}P)\ T_{ij} \neg + \sum \Delta T_{ijk}$

$T_{ij} \leftarrow$ update pixel

$\Delta T_{ij} \leftarrow$summation of all pixel

$K \leftarrow$ iteration

$P \leftarrow$ noise if present

Step 3.4 Predict the optimize difference of pixel

$$P_{ij} = \frac{(T_{ij}^{\alpha})(\eta_{ij}^{\beta})}{\sum_{z \varepsilon i}(T_{ij}^{\alpha})(\eta_{ij}^{\beta})}$$

$\propto \leftarrow$ x axis pixel, $\beta \leftarrow$y axis pixel

$\eta_{ij} \leftarrow$ predicted features

$P_{ij} \leftarrow$ updated features after prediction

Step 4: After feature extraction find optimize matching point combination by ACO

$$M_{ij} = \frac{(p_{ij}^{\alpha})(\eta_{ij}^{\beta})}{\sum_{z \varepsilon i}(P_{ij}^{\alpha})(\eta_{ij}^{\beta})}$$

Step 5: $M_{ij} \leftarrow$ matching points.

Step 6: Check these points if matching exist, image is copy otherwise not copy.

After the detection of copy move forgery using proposed methodology SIFT-ACO, Classification is performed for analyzing the performance of proposed technique.

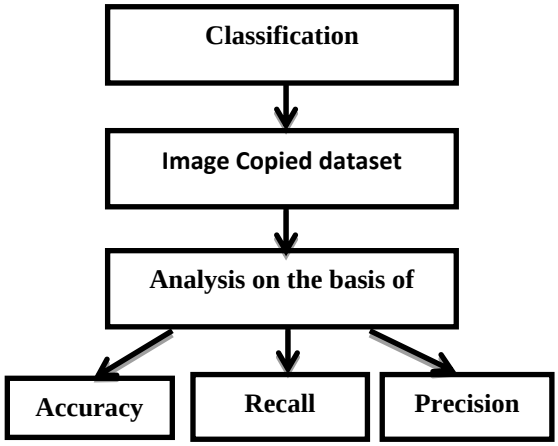

Fig. 3.2: Flow chart of Classification in Proposed Method

As presented in Fig. 3.2, classification is done by using extracted feature dataset from proposed SIFT- ACO technique with the help of supervised SVM classifier with polynomial Kernel. The analysis on the basis of accuracy, precision and recall is performed for proposed technique.

IV. RESULT AND ANALYSIS

In this paper two experiment setup, proposed SIFT-ACO method and existing SURF method has been implemented by utilizing MATLAB R2016a with image processing tool box.

4.1. Tampered Detection

In this paper Fig. 4.1and Fig. 4.2 show the experiment on proposed SIFT-ACO technique and existing SURF forgery detection technique where analysis of feature extracted or not is presented.

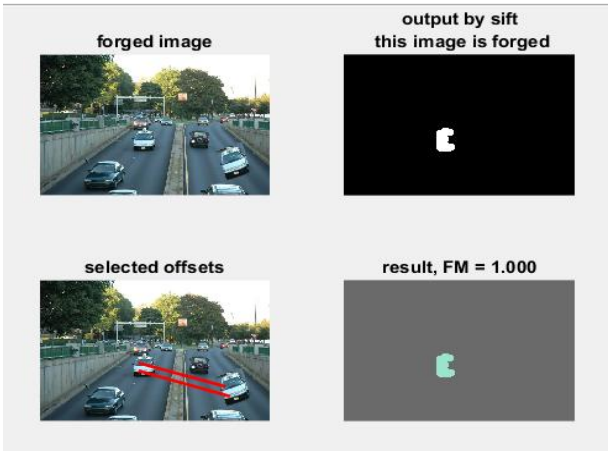

Fig. 4.1: Analysis of SIFT- ACO features Detection

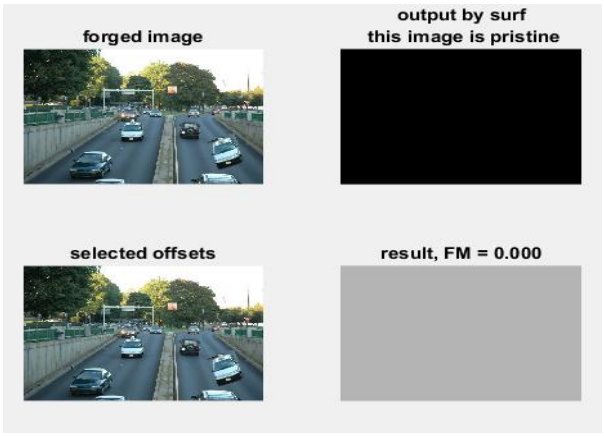

Fig. 4.2: Analysis of SuRF features Detection

Here, Detection results shows SURF features not able to detect forgery part in image but ACO optimization features detect using SIFT-ACO.

Table 4.1 Precision of different classifier

Classifier	**Precision**
SIFT with ACO (polynomial)	0.8917
SURF (Gaussian)	0.4714
SIFT with ACO (Gaussian)	0.9
SURF (polynomial)	0.4737

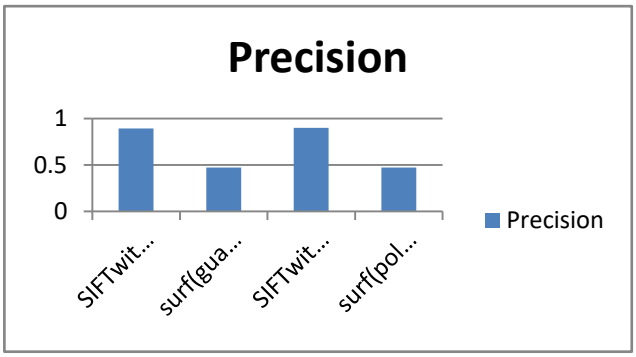

Fig. 4.3: Precision Graphs of different classifier

Here, different image forgery technique such as SIFT with ACO and SURF applied on roadmap image. From the results obtained it is found that SIFT with ACO has better precision as compared to other technique as shown in above Table and Fig. 4.3.

Table 4.2 Accuracy of different classifier

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

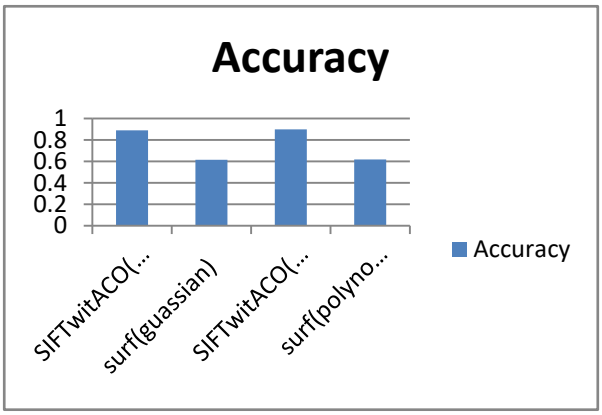

Fig. 4.4: Accuracy Graphs of different classifier

Here, result shows that SIFT with ACO shows better accuracy rate as compared to other technique as shown in Table and Fig. 4.4.

Table 4.3 Recall of different classifier

Classifier	**Recall**
SIFT with ACO(polynomial)	0.888
SURF(Gaussian)	0.4703
SIFT with ACO(Gaussian)	0.8963
SURF(polynomial)	0.4726

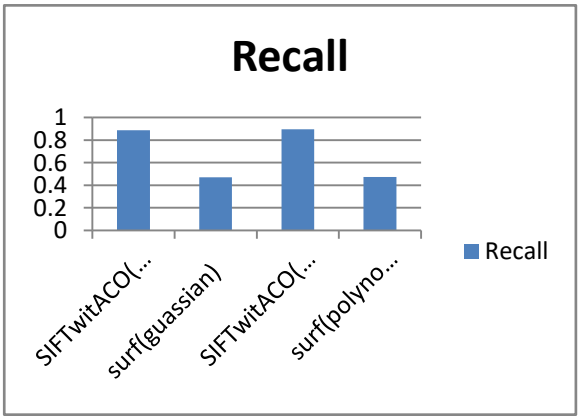

Fig. 4.5: Recall Graphs of different classifier

Here also seen that SIFT with ACO technique is good as compared to other technique as it also gives better recall rate as shown in Table and Fig. 4.5.

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 ACO(guassian)	0.9	0.8979	0.8963
SURF(polynomial)	0.4737	0.6193	0.4726

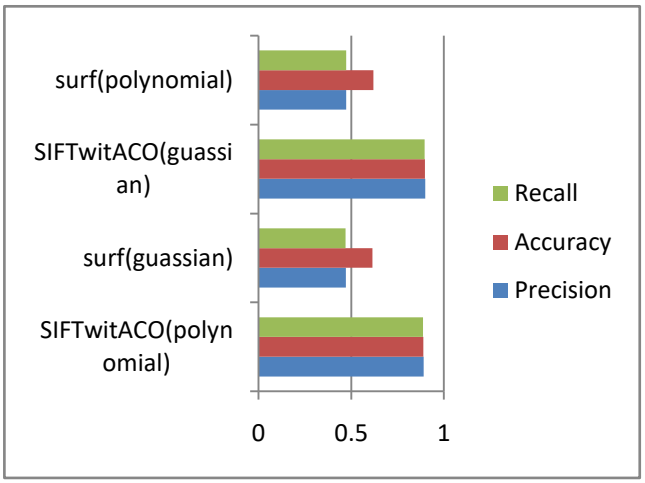

Fig. 4.6: Comparison Graph between parameters (Precision, Accuracy, Recall) of different classifiers

4.2. Classification

In classification COMFOD (copy move forgery dataset) and SVM classifier with Gaussian and polynomial Kernel is used. In above given fig 4.3,4.4, 4.5 and 4.6 experiment results on classification toolbox by support vector machine with two features set first is SIFT with ACO and latter is SURF feature by Gaussian and polynomial kernel shown. SIFT with ACO with polynomial kernel show significance high accuracy, precision and recall.

V. CONCLUSION

Copy-move forgery is a very common way to tamper an image. Sometimes the copied regions are rotated or flipped before being pasted. Many researchers have proposed various schemes to detect the tampered images. In this paper propose detection and classification method by using machine learning and optimization method. In our experiment detection and classification with SIFT ACO and SVM (Support Vector Machine) Gaussian and polynomial kernel is done. Result shows SIFT with ACO with polynomial kernel show significance high accuracy, precision and recall. So, SIFT with ACO outperform on another techniques.

REFERENCES

[1] G. Kang, Li, and Xiao-ping Cheng., "Copy-move forgery detection in digital image,'' Image and Signal Processing (ISP), 2010 3rd International Conferences on Vol.5.IEEE; 2010

[2] Singh, Sarvjit, Sunil Agrawal, and Gagandeep Singh, "ACCURACY Detection of Digital Image Forgery by using Ant Colony Optimization Technique," MATEC Web of Conferences. Vol.57. EDP Sciences 2016.

[3] Li, Weihai and Nenghai Yu., "Rotation robust detection of copy-move forgery," Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE 2010.

[4] Muhammad, Ghulam, Muhammad Hussain, and George Bebis, "Passive copy move image forgery detection using un-decimated dyadic wavelet transform," Digital Investigation 9.1 (2012): 49-57.

[5] Tralic, Dijana, "CoMoFoD—New database for copy-move forgery detection," ELMAR, 2013 55th international symposium. IEEE 2013.

[6] Khan, Saiqa, and Arun Kulkarni, "Reduced time complexity for detection of copy-move forgery using discrete wavelet transforms," International Journal of Computer Applications 6.7 (2010): 31-36.

[7] Zhang, Jing, Zhanlei Feng, and Yuting Su., "A new approach for detecting copy-move forgery in digital images," Communication Systems, ICCS2008. 11th IEEE Singapore International Conference on 2008.

[8] Li, Weihai, and Nenghai Yu., "Rotation robust detection of copy-move forgery," Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE 2010.

[9] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš, "Detection of copy-move forgery in digital images," In Proceedings of Digital Forensic Research Workshop, 2003.

[10] Thakur, Er. Neha, and Er. Bharat Batra, Color filter water drops algorithm for digital image forgery (copy move) detection.

[11] Li, Leida, "An efficient scheme for detecting copy-move forged images by local binary patterns," Journal of Information Hiding and Multimedia Signal Processing 4.1 (2013): 46-56.

[12] Lynch, Gavin, Frank Y. Shih, and Hong-Yuan Mark Liao, "An efficient expanding block algorithm for copy-move image forgery detection," Information Sciences 239 (2013): 253-265.