Block-Based Copy Move Forgery Detection Using Ant Colony Optimization

Malti Puri[1], Dr. Vinay Chopra[2]
[1,2]DAV Institute of Engineering & Technology
E-mail: [1]mp412141@gmail.com, [2]vinaychopra222@yahoo.co.in

***Abstract*—**In today's era due to the availability of wide range of inexpensive image capturing tools such as digital cameras, smart phones etc. there is a huge amount of digital images all over the world. Moreover, we have very inexpensive and easy to use photo editing tools such as Adobe Photoshop. So, it has become very easy to edit or manipulate an image. And any manipulation of a digital image is called digital image forgery provided it changes semantic of original image. Copy-move forgery is the most common type of digital image forgery. In this paper, we have proposed a new block-based copy-move forgery detection method that uses a metaheuristic approach i.e. Ant Colony Optimization to optimize the problem of copy move forgery detection. Ant colony optimization is basically used to optimize the performance of copy-move forgery detection system. Proposed system works by firstly taking a forged image as an input, the input image is converted from RGB color space to YCbCr color space. Then the YCbCr image is divided into non-overlapping blocks. Features from each block are extracted using Discrete Cosine Optimization (DCT) and are optimized using Ant Colony Optimization. At last matching between different blocks of the image is done using Ant Colony Optimization (ACO) to detect forgery. Matching regions are marked as forged regions and an output image is generated having forged regions marked. To evaluate the performance of proposed system experiments has been performed on images taken from two datasets: CoMoFoD and MICC-F2000. Experimental results of proposed system are very encouraging and were found to generate results with good Precision, Recall, f-measure (F1).

***Keywords*—** *Ant Colony Optimization; Digital image forgery; Copy-move forgery; CMFD.*

I. INTRODUCTION

In today's world due to the presence of low-cost and high-resolution digital cameras, there is a wide amount of digital images all over the world. Moreover, there are smartphones having high-resolution cameras. Therefore a huge amount of digital images are captured, stored and shared. Digital images play a very important role in various areas such as forensic investigation, surveillance systems, insurance processing, intelligence services, journalism, medical imaging etc. Also, there is a wide range of powerful, easy to use and cheap 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 the 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 the image etc. Sometimes forger may create forgery just to prove how smart he/she is or he/she can do so just for fun. Therefore it is necessary to check whether image is authentic or not [2].

A. *Copy-Move Forgery*

Copy-Move is a type of forgery in which a part of an 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 [9, 5]. So, the human eye usually has much more trouble detecting copy-move forgeries. Also, the 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.

B. *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. The authenticity of images cannot be neglected, especially when in the case of legal photographic evidence [10]. Digital images play a very important role in areas. Following are some important areas:

- Medical images are used in some areas to prove unhealthiness of a person or to claim that a person has a particular disease.
- In courtrooms, digital images are used as evidence and proofs against various crimes.
- In e- commerce sites images are an essential component. As images are used to display products and also are used to stand out from the crowd to attract customers.

C. *Digital Image forgery Detection Methods*

Digital image forgery detection techniques are mainly classified into two categories: one is active approach and another one is passive approach [2, 16]. See figure 1. The active approach requires a preprocessing step and suggests embedding of watermarks or digital signatures to images [16]. It relies on the presence of a watermark or signature and therefore requires 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 further retrieval of the watermark and examination of its condition indicates whether tampering has occurred. Whereas, in the case of passive approach forgery detection, there is no requirement of knowledge of original image. It does not rely on the presence of Digital watermark or Digital fingerprint. The passive approach is regarded as evolutionary developments in the area of tamper detection [16].

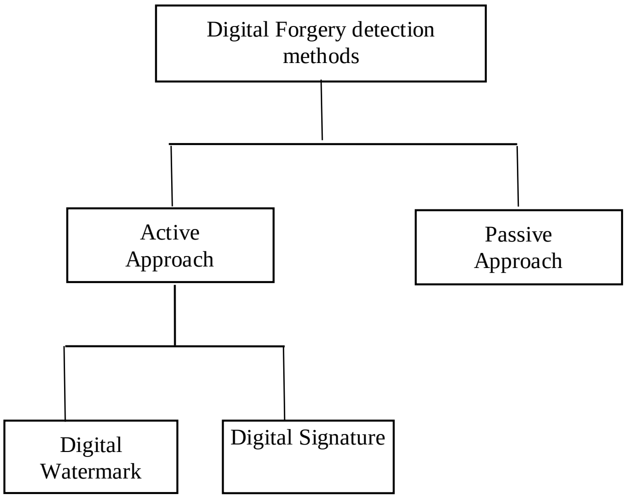


Fig.1 Digital image forgery detection methods [35]

D. Copy move forgery Detection Methods

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 2.

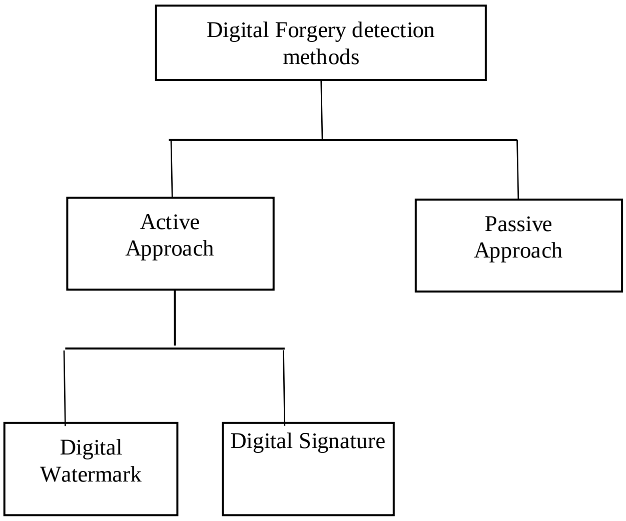


Fig.2 Digital image forgery detection methods [35]

E. Block Based Copy move forgery Detection

Block based method copy move forgery detection works by dividing the image into blocks. Features are extracted from each block and these blocks are compared to detect forgery. Higher the similarity between two blocks, higher is the chance that this block is copied. Block based copy move forgery detection technique works on pixel level [1]. Firstly the image is undergone pre-processing i.e. Converted from colored to grayscale or any other color space model. Pre-processing is optional. Then the image is subdivided into overlapping/non-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, correlation coefficient etc. There are a number of algorithms that according to the features that are selected for the feature extraction. Following are some important points about Block based method:

1. It works on the pixel level and gives detailed information about copied pixels.
2. It gives high accuracy.
3. The block-based method is slow and takes more time and more computational load for processing.
4. Works well in case of pure translation and also in the case of complex scenes.
5. Does not work well in case of geometric transformations.
6. Block base methods are insensitive to low-contrast regions.

Block-based copy move forgery detection method consists of six steps. Which are explained below:

Step 1: Input Image: First of all image to be tested is given as an input to the system.

Step 2: Preprocessing: Input image is undergone some kind of pre-processing operations such as converting image from RGB color space to grey scale or from RGB color space to YCbCr color space to reduce size needed to store the image.

Step 3: Block Tiling: After preprocessing image is divided into n number of overlapping or non-overlapping block of size mxm.

Step 4: Feature Extraction: Feature extraction is very important step in forgery detection. There are a number of features like Discrete Cosine Transform(DCT), Discrete Wavelet Transform (DWT), Local Binary Pattern (LBP), blur moments, HU, Zernike moments, Principle Component Analysis (PCA), Kernel Principle Component Analysis (KPCA) etc. which are classified under categories like Moments based, Intensity based, frequency based etc. [21].

Step 5: Feature Matching: Matching is done to detect the duplicated regions. High similarity between two feature descriptors depicts chances for a duplicated region. Matching can be done using lexicographic sorting, Best-Bin-First search etc. [21].

Step 6: Forgery detected: At last forged regions detected by feature matching are marked.

Jessica Fridrich et.al (2003) studied the problem of detecting the copy-move forgery and presented an efficient copy-move forgery detection method. A DCT-based method was proposed i.e. features were extracted using DCT. The method was proved to be reliable and efficient. It can successfully detect the forged regions even if the copied area is enhanced or retouched [10].

Babak Mahdian et.al (2006) proposed a method based on blur moment invariants to detect copy-move forgery. Firstly image divided into overlapping blocks. Each block is represented using blur moment invariants. To reduce the dimension of the blocks representation principal component transformation (PCA) is applied. After feature extraction feature matching is performed using a k–d tree .After matching forged regions are marked. The experimental results shows that proposed method is very efficient [2].

Er. Saiqa Khan et. al (2010) proposed a technique based on discrete wavelet transform(DWT) for detecting copied regions in copy move forgery. Firstly features are extracted by applying Discrete Wavelet Transform to the input image. Then block tiling is done to divide image into overlapping blocks. Feature matching is done using Phase Correlation and forged regions are detected. Experimental results proves that proposed approach has less computational time [7].

Seung-Jin Ryu et. al (2010) proposed a detection method of copy-move forgery using Zernike moments. Zernike moments' magnitude is invariant against rotation therefore proposed method is robust against rotation. It performs really well even in the presence of additive white Gaussian noise, JPEG compression, and blurring. However, does not work well if scaling operations or affine transformations are done in image [16].

Cao et al. (2012), present region duplication detection algorithm which depends on improved DCT and exhibits low computational complexity. The profound difference between this method and the other DCT-based methods is that here the quantized block is characterized by a circle block. The circle block is then divided into a fixed number of parts, for which the feature vectors are calculated. Euclidean distance between adjacent pairs is calculated after lexicographic sorting of vectors. This method is capable of identifying multiple region duplications and is also robust against blurring and additive noise but it has poor performance with poor image quality [5].

Leida Li et. al (2013) presents a new method for detecting the copy-move forgery. Focus of authors is to solve a main problem that many existing schemes fails to solve and the problem is when the copied region is rotated or flipped before being pasted. They proposed method based on Local Binary Pattern (LBP). Firstly image is divided into circular overlapping blocks. Local binary pattern features are extracted from circular blocks. At last feature vectors are compared to detect forged regions. LBP is rotation invariant hence proposed method is robust against rotation. Experimental results demonstrate that proposed method is robust against JPEG compression, noise, blurring and flipping [11].

Gavin Lynch et. al(2013) proposed an efficient expanding block algorithm. They basically enhanced the existing block based method and named it as efficient expanding block algorithm. Experimental results demonstrates that proposed method accurately detect forged area. Moreover, it can detect forgery even when postprocessing operations like JPEG compression or Gaussian blurring are done on image. It is mainly good at identifying the shape and the location of forged areas [8].

Zhao and Guo (2013), proposed a robust method to detect copy-move forgery based on DCT and SVD. The image is divided into fixed-size overlapping blocks and 2D-DCT is applied to each block. The DCT coefficients are then quantized to obtain a more robust representation of each block followed by dividing these quantized blocks into non overlapping sub-blocks. SVD is applied to each sub-block. Afterwards, features are extracted to reduce each block dimension using its largest singular value. Finally, feature vectors are lexicographically sorted, and the duplicated image blocks are matched by predefined shift frequency threshold. Experimental results showed that the proposed method can detect copy-move forgery even when an image was distorted by Gaussian blurring; Additive White Gaussian Noise (AWGN), JPEG compression or any other related mixed operations [21].

Guzin Ulutas et. al (2013) proposed a method based on Color Coherence. Color Coherence Vector (CCV) is used to determine the similarity among blocks in this method. The vector will designate the coherence of the colors in a region. Experiments show that the method can detect forged regions even if the image is processed by Gaussian Blurring to hide forgery [9].

Chi-Man Pun et. al (2015) proposed a new copy-move forgery detection scheme using adaptive over segmentation and feature point matching. The proposed scheme merge both block-based and Keypoint-based forgery detection methods. First, the proposed algorithm divides the input image into non-overlapping and irregular blocks. After that, the feature points (key-points) are extracted from each block as block features. These the block features are matched with one another to locate forged areas. The experimental results shows that the proposed method can give better results as compare to existing copy move forgery detection methods [6].

Shi Wenchang et. al (2016) proposed a method to implement Copy Move Forgery Detection with Particle Swarm Optimization (PSO). Proposed methods works by applying Particle Swarm Optimization (PSO) algorithm to the SIFT-based copy-move forgery detection method. Values of parameters needed in the forgery detection system are generated with the help of Particle Swarm Optimization. Experimental results of the proposed method gives positive results [17].

Beste Ustubioglu et. al (2016) proposed a method to detect copy-move forgery that can calculate threshold automatically. Threshold is value that is used to compare similarity between feature vectors. Authors uses DCT-phase terms to limit the range of the feature vector elements. Benford's generalized law is used to determine the compression history of the input. Unlike existing forgery detection methods the proposed method uses element-by-element equality between the feature vectors. Whereas other methods uses, of Euclidean distance or cross correlation. Experimental results show that the method can detect forged regions with higher accuracy ratios and lower false negative compared to existing methods [3].

II. AN OVERVIEW OF TECHNOLOGIES USED

A. Discrete Cosine Transform

Discrete cosine transform divides an image into sub bands called cosine functions and represents an image as oscillating at different frequencies. Cosine functions are also known as sinusoids and they vary in magnitude and frequency. DCT has application in various area of image processing such as image compression, video compression etc. because DCT has a special property that for an image visually significant data can be represented using some coefficient only. DCT uses real numbers only. There are basically eight standard DCT variants and only four are four are common out of the standard eight variants.

DCT Transforms image into to frequency domain from spatial domain. In frequency domain it can be efficiently encoded. It discards high frequency sharp variations components and thus refines the details of the image. DCT Focuses on the low frequency "smooth variations", holds the base of an image. It also removes redundancy between neighboring pixels. It provides the best compression ratio. Prepares image for quantization. Quantization is the step during which image is separated into the parts of different frequencies. Less important frequencies are discarded and most important frequencies that remain are used. Hence DCT can pack most information in fewest coefficients [7]. In the DCT algorithm the input image is divided into blocks of size 8x8 or 16x16, DCT coefficient is computed for each block, DCT are then quantized, then quantized coefficients are decoded and corresponding to each bock inverse (IDCT) is computed and at a last is stored as a single image [7]. It can detect the forgery even when the copied area is retouched and even when image is in saved in a lossy format.

B. 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 [41]. 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 [8, 41]:

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.

III. PROPOSED SYSTEM

After carefully analyzing we choose block-based method for our study. For feature extraction step Discrete Cosine Transform (DCT) is used. Features will be extracted using Discrete Cosine transform (DCT). Many researchers has used DCT while implementing Block-Based Copy-Moe Forgery detection systems. Ant Colony Optimization (ACO) is used to optimize the Copy-move forgery detection system. ACO will be used for feature extraction and feature matching step. First features will be extracted using DCT, then feature extraction will be optimized using ACO.

```
Algorithm: ACO based Copy move forgery detection
Input: Forged Image;
Output: Image with detected forged regions
Begin
    1. Take a colored forged image as input;
    2. Convert image into YCbCr;
    3. Divide YCbCr image into overlapping blocks;
    4. Store these blocks into a metrics;
    5. Initialise ants;
    6. While not termination condition do
    7. Update Pixel;
    8. Predict Features;
    9. End While;
    10. If matching Image copied output the final result;
End
```

The proposed methodology is implemented using MATLAB 2016a. The experimentation is done on various forged images taken from CoMoFoD and MICC-F2000 Dataset, which is available online.

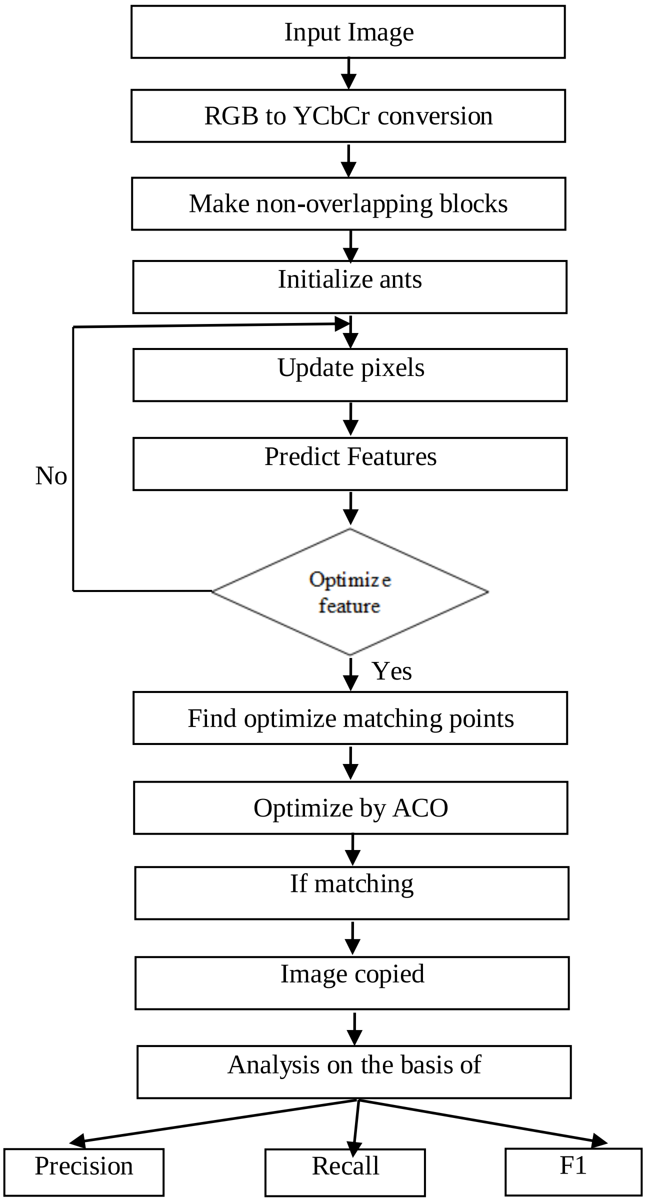


Fig.3 The architecture of the algorithm

Step 1 In first step image is converted into YCbCr space from RGB to reduce size of the image.

Step 2 After converting image into YCbCr color space, block-tiling is done, Image is divided into overlapping blocks. Block size is taken to be 8×8. Each block of an image of size N×M is denoted as Bi. Where i=1, 2…. (N-7) (M-7).

Step 3 Features are extracted using DCT phase and further feature extraction is optimized using ACO. Ants are initialized and pheromones deposited by ants, and they traverse from one node to another. Feature is represented by node here. Pheromone is updated according to the formula:

$$p_{ij}^{k} = \frac{\tau_{ij}^{\alpha} \cdot \eta_{ij}^{\beta}}{\sum_{l \in N_i^k} \tau_{il}^{\alpha} \cdot \eta_{il}^{\beta}} \qquad (1)$$

Where i=0,1,….n.
∝ 🡐 x axis pixel, β 🡐 y axis pixel
η_{ij}🡐 predicted features
P_{ij} 🡐 updated features after prediction

STEP 4 Feature Matching is also done with the help of ACO. Formulae used for updating pheromone values is:

$$p_{ij}^{k} = \frac{\tau_{ij}^{\alpha} \cdot \eta_{ij}^{\beta}}{\sum_{l \in N_i^k} \tau_{il}^{\alpha} \cdot \eta_{il}^{\beta}} \qquad (2)$$

Step 5 Mark the forged regions.
Step 6 Analysis on the basis of Precision, Recall, F1.

IV. Result and Analysis

The proposed method is implemented in MATLAB 2016a. To test efficiency of the proposed system different parameters Precision, Recall and F1 are used. F1 also known as F-Measures. Experimentation is done on images taken from dataset CoMoFoD and MICC-F2000 that is available online.

Precision denotes the probability that a detected forgery is truly a forgery. Formula of Precision is given by equation 3.

$$\boldsymbol{Precison} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \qquad \textbf{(3)}$$

Where TP is True positive i.e. number of correctly detected images. FP is false Positive i.e. number of falsely detected forged regions.

Recall shows the probability that a forged image is detected. Formula of Recall is given by equation 4.

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \qquad \textbf{(4)}$$

Where TP is True positive i.e. number of correctly detected images.

FN is false negative i.e. number of falsely missed regions.

F-measure is the addition of both Recall and Precision. Formulae is given by equation 5.

$$\textbf{F-measure=}\ 2.\frac{\boldsymbol{Precision\ .Recall}}{\boldsymbol{Precision+Recall}} \qquad \textbf{(5)}$$

The above methodology is implemented in MATLAB 2016a. Experimentation is done on images taken from dataset CoMoFoD and MICC-F2000 that is available online.

Experimental results of some images is given below:

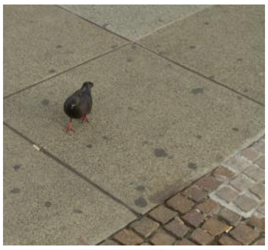


Fig. 4 Original Image

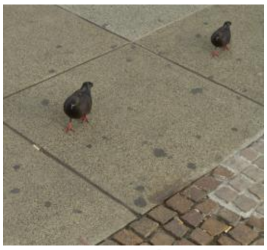


Fig. 5 Forged Image (Input Image)

Figure 4 is original image having one bird. Figure 5 is created by copying bird and pasting it over another part of the same image.

To detect forgery using proposed system figure 5 i.e. the forged image will be given as input. Image will undergone various processing steps and at the end forged regions will be marked and an output will be generated. Output generated at each step is shown as following:

Step 1 RGB to YCbCr Conversion

Figure 6 shows the input image after its conversion into YCbCr color space from RGB color space.

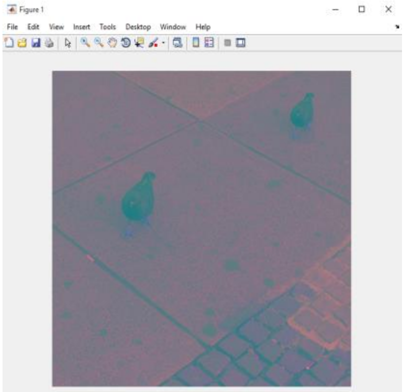


Fig. 6 RGB to YCbCr of forged Image

Figure 7 also shows the YCbCr of input image. But it displays the different components i.e. Y component, Cb component and Cr component of input forged image.

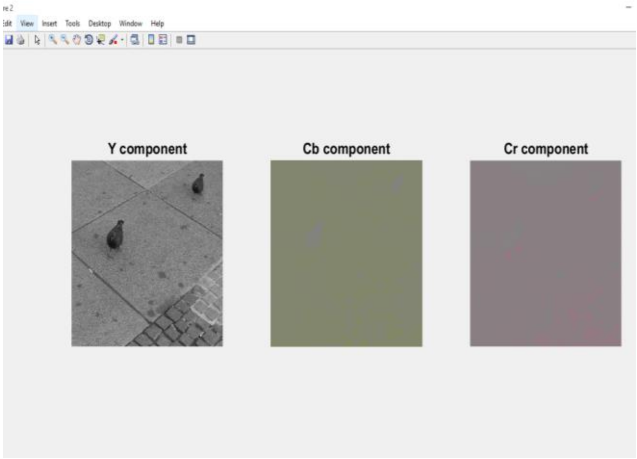


Fig. 7 Y, Cb & Cr component of forged image

Step 2 Block Tiling

Figure 8 shows the image after block tiling. It clearly illustrates image as non-overlapping blocks.

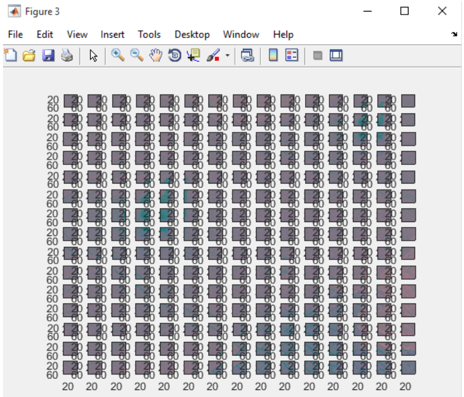
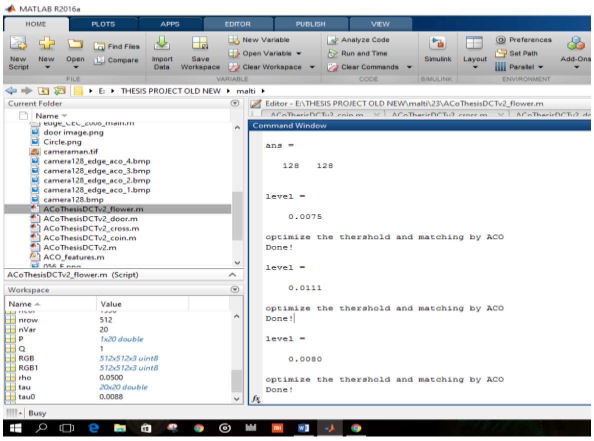


Fig. 8 Block tiling of input image

Step 3 Value of threshold

In proposed work threshold will be calculated automatically. And this value will be used to detect forgery. Figure 9 shows this step.



Name	Value
nrow	512
nVar	20
P	1x20 double
Q	1
RGB	512x512x3 uint8
RGB1	512x512x3 uint8
rho	0.0500
tau	20x20 double
tau0	0.0088

```
ans =

   128   128


level =

    0.0075

optimize the thershold and matching by ACO
Done!

level =

    0.0111

optimize the thershold and matching by ACO
Done!

level =

    0.0080

optimize the thershold and matching by ACO
Done!
```

Fig. 9 Threshold Calculation

Step 4 Feature extraction and Feature Matching using Ant Colony Optimization (ACO)

Feature extraction and feature matching is the main step in any copy-move forgery detection system. In proposed work feature extraction and matching is being optimized using ant colony optimization. ACO Graph is shown in figure 10.

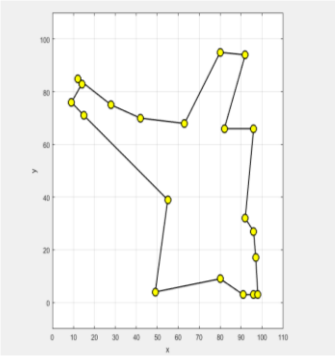


Fig.10 Iteration graph

Step 5 Forgery Detected

In the last step we will get an output displaying detected forged regions. Fig. 11 illustrates the final output that we get using proposed system.

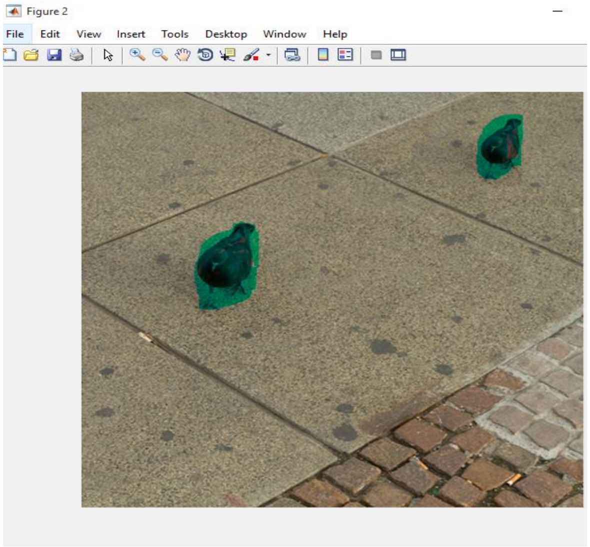


Fig.11 Detected Forged regions

Figure 12 depicts a graph that shows values of parameters used in study i.e. Precision, Recall and F1 corresponding to input forged image.

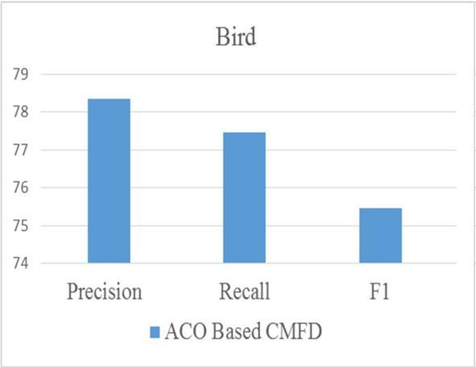


Fig. 12 Parameter values of Proposed CMFD

Experimentation is done on different images to evaluate the proposed system on the basis of parameters: Precision, Recall, F1. Results of those images are discussed next.

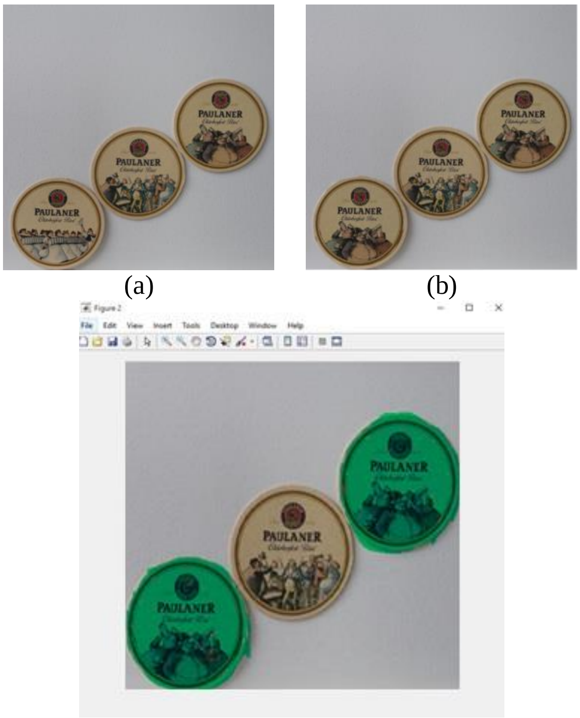


Fig. 13 (a) Original image, (b) forged image, (c) Detected forged regions

Figure 13(a) is original image,Figure 13(b) if copy-move forged image that is given as input, and we will get Figure 13(c) as final output with detected forged region

Figure 14 depicts a graph that shows values of parameters used in study i.e. Precision, Recall and F1 corresponding to input forged image.

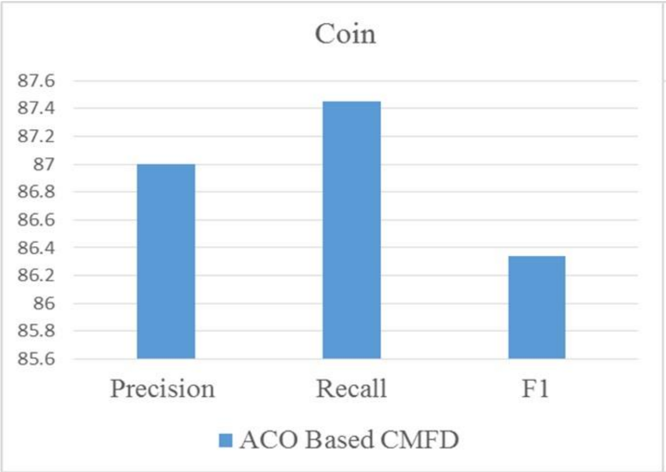


Fig. 14 Parameter values of Proposed CMFD

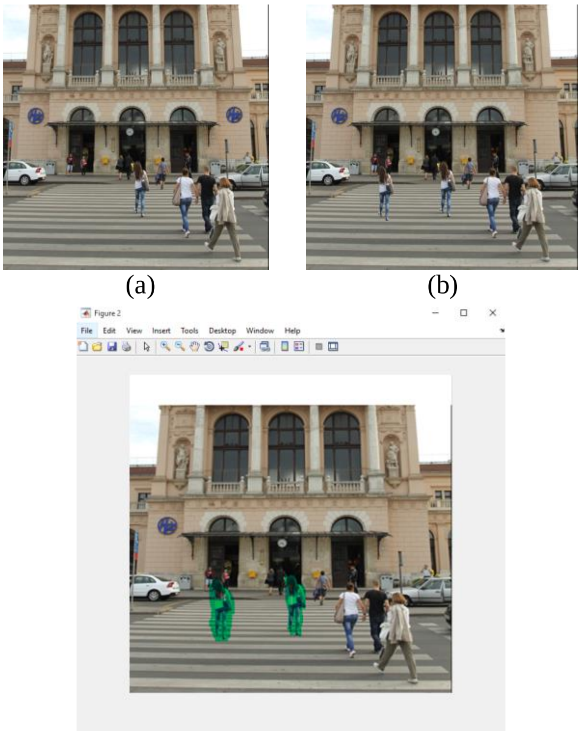


Fig. 15 (a) Original image, (b) forged image, (c) Detected forged regions

Figure 15(a) is original image,Figure 15(b) if copy-move forged image that is given as input, and we will get Figure 15(c) as final output with detected forged region

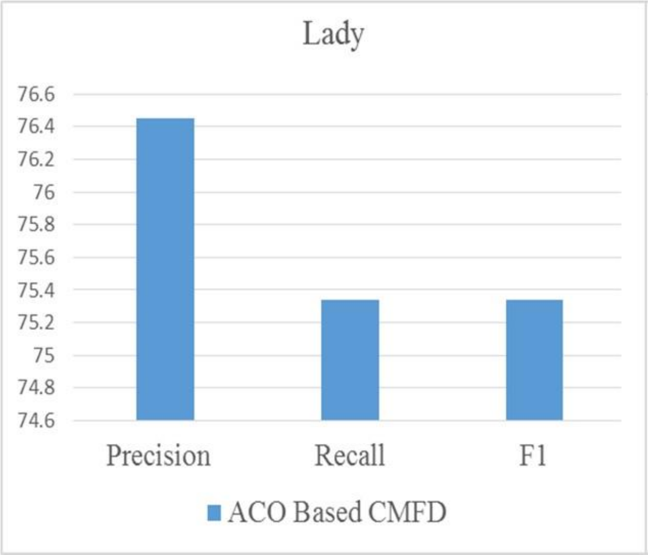


Fig. 16 Parameter values of Proposed CMFD

Figure 16 depicts a graph that shows values of parameters used in study i.e. Precision, Recall and F1 corresponding to input forged image.

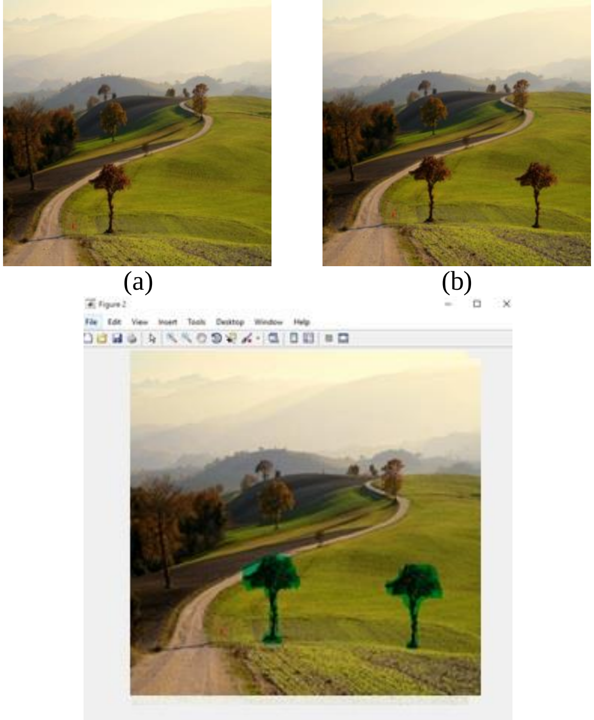


Fig. 17(a) Original image, (b) forged image, (c) Detected forged regions

Figure 17(a) is original image,Figure 17(b) if copy-move forged image that is given as input, and we will get Figure 17(c) as final output with detected forged region.

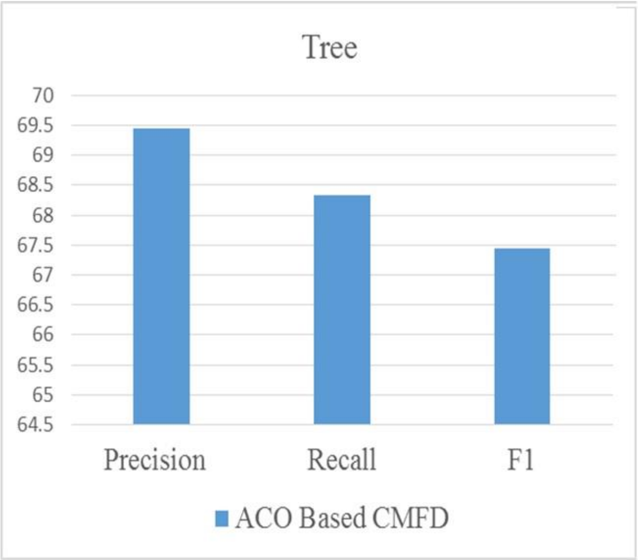


Fig. 18 Parameter values of Proposed CMFD

Figure 18 depicts a graph that shows values of parameters used in study i.e. Precision, Recall and F1 corresponding to input forged image.

V. CONCLUSION

Digital images have become integral part of day to day life and are used to present important information. Digital image forgery is very common these days with the availability of editing tools. So, authenticity of image has become major concern.

In this study we have designed a block based copy-move forgery detection system using Ant Colony Optimization. Ant colony optimization is basically used to optimize the performance of copy-move forgery detection system. Proposed system works by firstly taking a forged image as an input, input image is converted from RGB color space to YCbCr color space. Then YCbCr image is divide into non-overlapping blocks. Features are extracted using Discrete Cosine Optimization (DCT) and are optimized using Ant Colony Optimization. At last matching between different blocks of image is done using Ant Colony Optimization (ACO). Matching regions are marked as forged regions and an output image is generated having forged regions marked. Experiments are done on a database of images to evaluate the performance of the proposed system. These images were selected from two datasets: CoMoFoD and MICC-F2000, which is available online. Experimental results of proposed system are very encouraging.

Currently there are a number of techniques to detect copy- move forgery. We have optimized using Ant Colony Optimization. Further research can be extended as:

1. Graphical user interface for the system.
2. Provision to counter postprocessing operations.
3. Can be integrated with other methods such as DWT, PCA, LBP etc.

Work can be implemented on videos to search for duplicated blocks to perform on multiple image frames.

ACKNOWLEDGMENT

I would like to express my gratitude to Dr. Vinay Chopra for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

VI. REFERENCES

[1] Alin C Popescu and Hany Farid, "Exposing digital forgeries by detecting duplicated image regions,"Department of Computer Science, Dartmouth College,Tech. Rep. TR2004-515, pp. 1-11, 2004.

[2] Babak Mahdian , Stanislav Saic," Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, an international journal dedicated to the applications of medicine and science in the administration of justice, Vol.171 No.2-3 , pp. 181-189, .2007.

[3] Beste Ustubioglu, Guzin Ulutas , Mustafa Ulutas, Vasif V. Nabiyev," A new copy move forgery detection technique with automatic threshold determination", Elsevier - International Journal of Electronics and Communications Volume 70, Issue 8, pp. 1076–1087, August 2016.

[4] Bolun Chen , Ling Chen , Yixin Chen, "Efficient ant colony optimization for image feature selection",Volume 93, Elsevier-Special issue on Machine Learning in Intelligent Image Processing, Issue 6, June 2013, pp. 1566–1576.

[5] Cao Y, Gao T, Fan L, Yang Q,"A robust detection algorithm for copy-move forgery in digital images",Elsevier: Forensic Sci Int. 2012 pp.33-43.

[6] 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.

[7] Er. Saiqa Khan, Er. Arun Kulkarni," An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010,pp.1801-1806.

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

[9] Guzin Ulutas, Mustafa Ulutas, "Image forgery detection using Color Coherence Vector", Electronics, Computer and Computation (ICECCO), Nov. 2013, pp. 107 – 110.

[10] Jessica Fridrich, David Soukal and Jan Lukas, "Detection of copy–move forgery in digital images", Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, August 2003, pp. 55–61.

[11] Leida Li, Shushang Li, Hancheng Zhu,"An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns",Journal of Information Hiding and Multimedia Signal Processing,Volume 4, Number 1 ,January 2013, pp46-56.

[12] Malti Puri, Dr. Vinay Chopra ," A Review: Block-Based Copy-Move Forgery Detection Methods ", Volume 5, Issue 10, October - 2016.

[13] M. K. Bashar, K. Noda, N. Ohnishi, H. Kudo, T. Matsumoto, and Y. Takeuchi, "Wavelet-Based Multiresolution Features for Detecting Duplications in Images",IAPR Conference on Machine Vision Applications, 2007,pp. 264-267.

[14] Mehdi Hosseinzadeh Aghdam *, Nasser Ghasem-Aghaee, Mohammad Ehsan Basiri, "Text feature selection using ant colony optimization", Elsevier: Expert Systems with Applications 36 ,2009, pp. 6843–6853.

[15] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour,"Iterative Copy -Move Forgery Detection Based on a New Interest Point Detector",IEEE Transactions on Information Forensics and Security,2016, pp.1-14.

[16] Seung-Jin RyuMin-Jeong LeeHeung-Kyu Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments",Springer: Information Hiding. IH 2010. Lecture Notes in Computer Science, vol 6387, pp.51-65

[17] 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.

[18] Vincent Christlein, Johannes Jordan "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on information forensics and security, 2012, pp. 1-26.

[19] Xiaomei Quan, Hongbin Zhang, "Copy-Move Forgery Detection in Digital Images Based on Local Dimension Estimation" Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) International Conference, June 2012, pp.180-185.

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

[21] Zhao J1, Guo J., "Passive forensics for copy-move image forgery using a method based on DCT and SVD" ,Elsevier: Forensic Sci Int. 2013,pp.158-166.