Detection of Image Forgeries Using Ant Colony Optimization (ACO) Methodology

[1]Ms. Bindhu A, [2]Ms. Dhanusha A

[1]Assistant Professor, [2]PG Scholar
Department of Computer Science and Engineering,
Marthandam College of Engineering and Technology, Kuttakuzhi, India

***Abstract*: Now-a-days, digital images have acquired the reputation of being an important evidence. However, with the development of imaging technology and the accessibility of powerful affordable image editing tools like Photoshop, it is becoming easier to add, modify or remove important features from an image without leaving any visual traces. Any image manipulation can become a forgery, based upon the context in which it is used. Thus today digital images are losing authenticity and it is becoming difficult to distinguish between authentic and tampered images; which is an essential requirement in various areas like in legal cases, in electronic media, in medical profession, and in research works etc. Copy move is the most common technique used for creating digital image forgeries in which a part of an image is copied and pasted elsewhere in the same image. Due to the technology advancement and availability of lots of sophisticated image editing tools, the digital images are losing authenticity. This has led to the proposal of different detection techniques to check whether the digital images are authentic or forged. Copy move forgery is a special type of forgery technique whose detection has become a widely used research topic under digital image forensics. The proposed system implement the feature extraction using principle component analysis and optimization (ant colony optimization) algorithm to detect the forgery image in JPG images. In optimization approach to classify the features and match the training feature if training and testing features has matching then detect the forgery image in the jpg images.**

***Keywords*: Image Forgery, Copy Move Detection, Digital Image Editing, Ant Colony Optimization**

1. INTRODUCTION

The detection image forgery has become very difficult as manipulated images are often visually indistinguishable from real images. With the advent of high-tech image editing tools, an image can be manipulated in many ways. The types of image manipulation can broadly be classified into two categories: (1) content-preserving, and (2) content-changing. The first type of manipulation (e.g., compression, blur and contrast enhancement) occurs mainly due to post-processing, and they are considered as less harmful since they do not change any semantic content. The latter type (e.g., copy-move, splicing, and object removal) reshapes image content arbitrarily and alters the semantic meaning significantly. The content-changing manipulations can convey false or misleading information. As the number of tampered images grows at an enormous rate, it becomes crucial to detect the manipulated images to prevent viewers from being presented with misleading information. Recently, the detection of content-changing manipulation from an image or a video has become an area of growing interest in diverse scientific and security/surveillance applications. Digital image forgery is classified into two categories. One is copy-move forgery and the other is copy-create forgery. When images are forged by copying one part of image and pasted on another part it is known as copy move forgery. While in case of copy-create forgery copying and pasting is done by using more than just a single image. The proposed system deals with the copy move forgery only. It employs Ant colony optimization (ACO) methodology which is used to detect y the copy-move forgery. ACO is the intelligence technique used by the ants to find their food. When ants move randomly in order to find the shortest path between the source of food and their colony, they deposit pheromone along the path. Pheromone is a source of communication between them. An ant can do only simple tasks but not the complex tasks like searching shortest path from nest to food source. F is the food source at some distance from nest, N and after finding food they come back by path, (b) after leaving pheromone trail by an ant. At the start, all the ants move along all the possible paths but the pheromone intensity is strong for the shorter path than the longer path. Most of the ants follow the shortest path route from the nest to the food source; the pheromone trails on the other paths are lost. This intelligence technique is implemented in ACO to detect image forgery.

II. RELATED WORKS

Jawadul H. Bappy et al., proposed system is a high-confidence manipulation localization architecture that utilizes resampling features, long short-term memory (LSTM) cells, and an encoder–decoder network to segment out manipulated regions from non-manipulated ones. Resampling features are used to capture artifacts, such as JPEG quality loss, upsampling, downsampling, rotation, and shearing. The proposed network exploits larger receptive fields (spatial maps) and frequency-domain correlation to analyze the discriminative characteristics between the manipulated and non manipulated regions by incorporating the encoder and LSTM network. Weiqi Luo et al., describes an efficient and robust algorithm for detecting and localizing this type of malicious tampering. Maryam Jaberi et al., introduces the process of detecting duplicated regions in an image by exploiting the similarity between keypoint-based features in these regions. In this paper, we have adopted keypoint-based features for copy–move image forgery detection; however, our emphasis is on accurate and robust localization of duplicated regions. It is proposed using a more powerful set of key point based features, called MIFT, which shares the properties of SIFT features but also are invariant to mirror reflection transformations. Lamberto Ballan et al., introduces a novel methodology based on Scale Invariant Features Transform (SIFT) is proposed. Such a method allows both to understand if a copy-move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. Wenjun Lu et al., proposes a new framework to perform multimedia forensics by using compact side information to reconstruct the processing history of a multimedia document. E. Ardizzone et.al. In this paper creators displayed an exceptionally novel half and half approach, which thinks about triangles rather than contrasting pieces or single focuses. Intrigue focuses are extricated from the picture and questions are demonstrated as an arrangement of associated triangles utilizing these focuses. Triangles are coordinated by their shapes, their substance, and the neighborhood includes vectors removed onto the vertices of the triangles. Proposed strategy is intended to be hearty to geometric transformations. Results were contrasted and a piece coordinating strategy and a point-based technique. Chi-Man Pun et.al. In this paper creators proposed a novel copy-move forgery detection conspire to utilize versatile over division and highlight point coordinating. The proposed plot coordinates both block-based and Keypoint-based forgery detection strategies. To begin with, the proposed versatile over division calculation sections the host picture into nonoverlapping 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.

III. PROPOSED SYSTEM

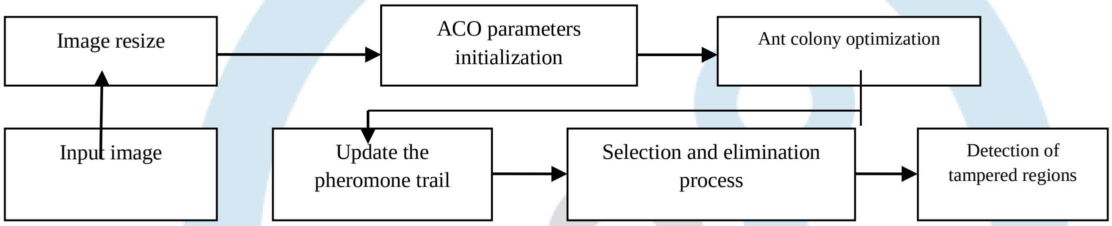


Image resize
ACO parameters initialization
Ant colony optimization
Input image
Update the pheromone trail
Selection and elimination process
Detection of tampered regions

Fig 1: Block Diagram

The proposed system is to localize the manipulated regions at a pixel level. Digital image forgery is classified into two categories. One is copy-move forgery and the other is copy-create forgery. When images are forged by copying one part of image and pasted on another part it is known as copymove forgery. While in case of copy-create forgery copying and pasting is done by using more than just a single image. The proposed system deals with the copymove forgery only. It have employed Ant colony optimization (ACO) methodology which is used to detect the copy-move forgery. ACO is the intelligence technique used by the ants to find their food. When ants move randomly in order to find the shortest path between the source of food and their colony, they deposit pheromone along the path. Pheromone is a source of communication between them. An ant can do only simple tasks but not the complex tasks like searching shortest path from nest to food source. F is the food source at some distance from nest, N and after finding food they come back by path, (b) after leaving pheromone trail by an ant. At the start, all the ants move along all the possible paths but the pheromone intensity is strong for the shorter path than the longer path. Most of the ants follow the shortest path route from the nest to the food source; the pheromone trails on the other paths are lost. This intelligence technique is implemented in ACO to detect image forgery.

IV. METHODOLOGY

- Image resize

Firstly it load the images of size M×N in for execution which are already stored in some databases. Image interpolation occurs when you resize or distort your image from one pixel grid to another. Image resizing is necessary to increase or decrease the total number of pixels, whereas remapping can occur when you are correcting for lens distortion or rotating an image. Interpolation works by using known data to estimate values at unknown points. Image interpolation works in two directions, and tries to achieve a best approximation of a pixel's intensity based on the values at surrounding pixels. It includes the following processes.

- ACO initialization
  - Initializing ACO parameters to given number of iterations and search area.
- Ant colony optimization

- Block construction

Step 1: Firstly it load the images of size M×N in MATLAB environment which are already manipulated from some databases.

Step 2: Initializing ACO parameters to given number of iterations and search area. These parameters are ant population (which is 200), steps for the random movement of ants and search area in which random movement is allocated within the image.

Step 3: Initializing Ants population, we took ant as a location on which forgery is detecting .Here ant has two locations, one for x and another for y. X & Y corresponds to rows and columns with in the search limit (X×Y). From every location, every ant represents a block called ant block denoted by (K).

Step 4: After that we divide image into equal square blocks of size m×m within the search limit called current block denoted by (I).

Step 5: Randomly distribution of ants with in the search area and random movement given by them for generating and searching for food values at different locations.

Step 6: Nutrient function

$$\sum_{i=1}^{m}\sum_{j=1}^{m}(|I_{i},j - K_{i},j|)_{R} + \sum_{i=1}^{m}\sum_{j=1}^{m}(|I_{i},j - K_{i},j|)_{G} + \sum_{i=1}^{m}\sum_{j=1}^{m}(|I_{i},j - K_{i},j|)_{B}$$

Where R, G and B denotes the subtraction for Red, Green and Blue matrices present in both current and ant block.mAnd predict food value using the above nutrient function.

Step 7: The selection and elimination process exchanges the food locations among ants.

Step 8: Process will continue for next N iterations. In this way, minimum will be difference between the current block and ant block higher will be the probability

of forgery. The analysis of an image using above mentioned technique promises the detection of tampered regions present in the input image.

Pseudocode for ACO

```
Begin;
Initialize the pheromone trails and parameters; Generate population of m solutions (ants);
For each individual ant k to m: Calculate fitness (k);
For each ant determine its best position; Determine the best global ant;
Update the pheromone trail;
Check if termination Z true;
End;
```

V. EXPERIMENTAL RESULTS

The following are the snapshots of results on execution of the program considering different cases are shown below. This system was implemented in MATLAB 2013 software in windows environment. In order to execute the prototype the datasets NIST’16 is used to verify the system, it includes three main types of manipulation (a) copy-clone, (b) removal, and (c) splicing.

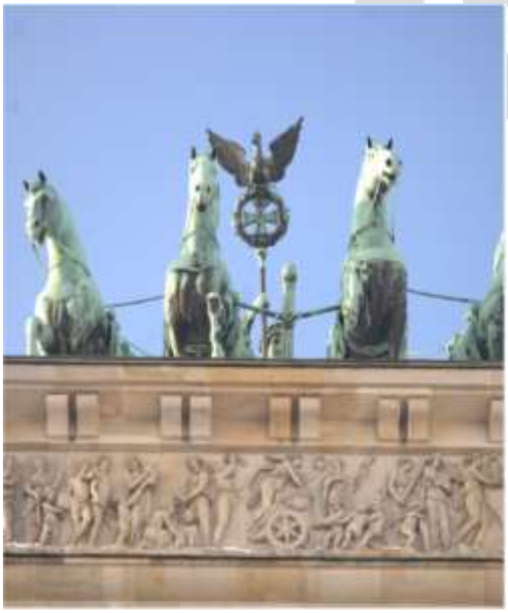


Fig 2 Input Image

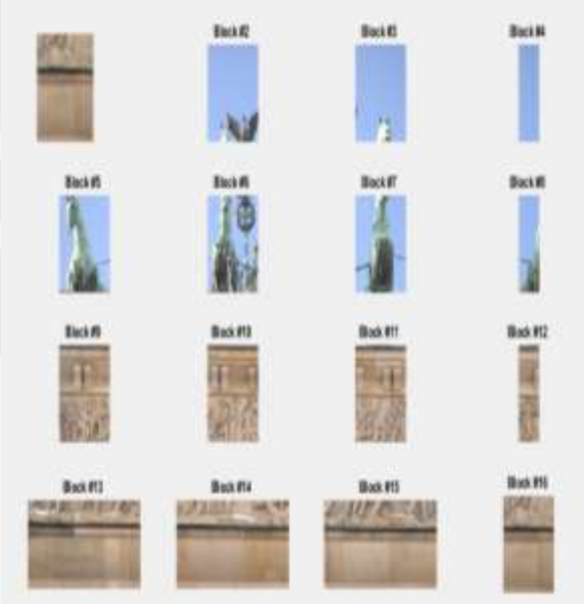
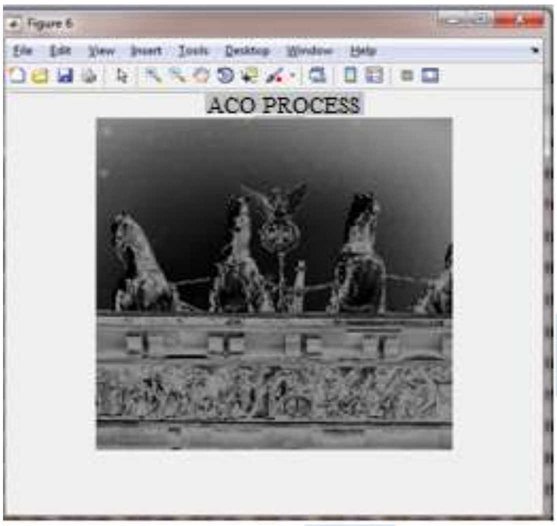


Fig 3 Mutiscale Patch Extraction

The fig 2 display’s the selected input image. It is applied with different processing to predict the image forgeries. The fig 3 is used to display the patch construction module, it first extract non-overlapping patches. As input image has size of 256x256, Then, the square root of magnitude of 3 × 3 Laplacian filter is used to produce the magnitude of linear predictive error for each extracted patch.



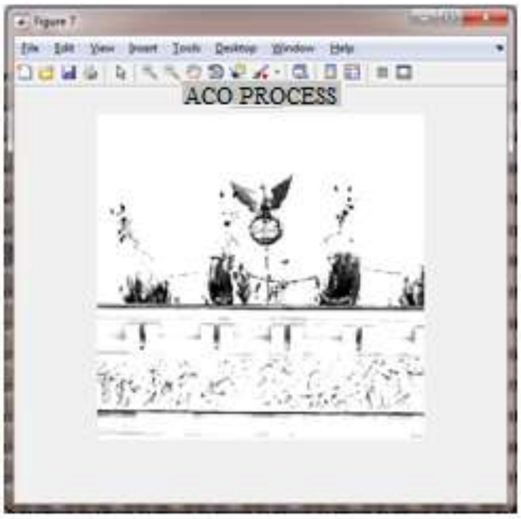


Fig 4 Ant colony optimization

Fig 5 Ant colony optimization

The Fig 4 shows Ant colony optimization (ACO) methodology which is used to detect the copy-move forgery. ACO is the intelligence technique used by the ants to find their food. When ants move randomly in order to find the shortest path between the source of food and their colony, they deposit pheromone along the path. Pheromone is a source of communication between them. At the start, all the ants move along all the possible paths but the pheromone intensity is strong for the shorter path than the longer path. Most of the ants follow the shortest path route from the nest to the food source; the pheromone trails on the other paths are lost.

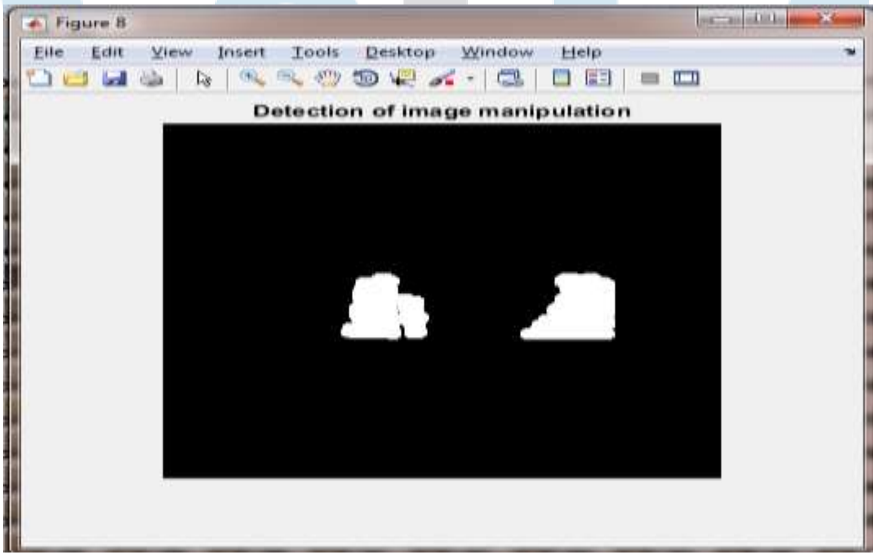


Figure 8
File Edit View Insert Tools Desktop Window Help
Detection of image manipulation

The Fig 4 shows the detected forgery in the input image.

CONCLUSION

The proposed system is a deep learning based approach to semantically segment manipulated regions in a tampered image. Digital image forgery detection is really complicated task in the present times because of the advancement of the new image editing tools. It is very difficult for an individual to detect the authenticity of an image by naked eyes. In order to improve the low detection rate of the forged regions in the digital photo image it have mentioned the intelligence technique (ACO) in the proposed system. The proposed method shows excellent detection of the tampered regions. The advantage of this approach is to find the manipulated areas present within the input image precisely and accurately. The proposed algorithm promises to expose the digital image forgery created by copy-move method.

REFERENCES

[1] O. M. Al-Qershi and B. E. Khoo, “Passive detection of copy-move forgery in digital images: State-of-the-art,” Forensic Sci. Int., vol. 231, no. 1, pp. 284–295, 2013.

[2] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A sift-based forensic method for copy–move attack detection and transformation recovery,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[3] M. D. Ansari, S. P. Ghrera, and V. Tyagi, “Pixel-based image forgery detection: A review,” IETE J. Educ., vol. 55, no. 1, pp. 40–46, 2014.

[4] V. Badrinarayanan, A. Kendall, and R. Cipolla, “SegNet: A deep convolutional encoder-decoder architecture for image segmentation,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 12, pp. 2481–2495, Dec. 2017.

[5] J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. Manjunath, “Exploiting spatial structure for localizing manipulated image regions,” in Proc. ICCV, Oct. 2017, pp. 4970–4979.

[6] B. Bayar and M. C. Stamm, “A deep learning approach to universal image manipulation detection using a new convolutional layer,” in Proc. 4th ACM Workshop Inf. Hiding Multimedia Secur., 2016, pp. 5–10.

[7] B. Bayar and M. C. Stamm, “Design principles of convolutional neural networks for multimedia forensics,” Electron. Imag., vol. 2017, no. 7, pp. 77–86, 2017.

[8] B. Bayar and M. C. Stamm, “On the robustness of constrained convolutional neural networks to jpeg post-compression for image resampling detection,” in Proc. 42nd IEEE Int. Conf. Acoust., Speech Signal Process., Mar. 2017, pp. 2152–2156.

[9] A. Bharati, R. Singh, M. Vatsa, and K. W. Bowyer, “Detecting facial retouching using supervised deep learning,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 9, pp. 1903–1913, Sep. 2016.