ACCURACY Detection of Digital Image Forgery by Using Ant Colony Optimization Technique

Sarvjit Singh [1, a], Sunil Agrawal[1] and Gagandeep Singh[1]

[1] *ECE Department, UIET Panjab University, Chandigarh, India*

Abstract. Image forgery is one of the well known fields in which researches continuously exploring new areas. In digital image forgery one can change image in many ways using several software's, researchers exploring new algorithms to detect image forgery areas and change it to original pixel values if possible. In this paper we employed ACO (Ant Colony Optimization) to find areas which are manipulated with some software. The experimental results prove that ACO is better than existing methods of detecting tampered regions in digital photo images.

Keywords - ACO, digital photo image, digital forgery, digital image forensics.

1 Introduction

In these days, with the advancement of digital image processing methods, it is very easy for anyone to tamper the digital images and hide the objects or manipulate the objects present in the digital photo image. This is possible due to the development of sophisticated image editing tools. Tampered images has great effect on our society because images are everywhere in our life such as magazines, news images, the images produced as court evidence and medical diagnostic etc. so in order to know that the images are authentic or unauthentic we need digital image forensics which are used to detect the tampered regions present in the digital photo images. For the last few years, digital image forensics becomes more attentive to restore the lost trust of digital photo images. That is why it is a great need to develop the methods for the digital image authentication in order to recover the confidence of people towards the digital photo images. There are two techniques to detect the digital image forgery.

One is active based approach and the other one is passive based approach. The active based approach is further divided into digital watermarks and signatures. Digital watermarking and signatures methods for the detection of tampered regions in the images has been used in the past times but for these methods we have to preprocess the data first, which creates difficulty to apply these methods [1].

Other approach is passive based. In this method we do not need any information about the image itself. In this approach in order to detect the suspicious regions we need to extract some intrinsic characteristics traces present in the digital photo image. We detect the tampered region by using the forged image as an input. For this reason passive based approach is most preferred.

Moreover, active based approach requires extra operations and harms the original image so passive based approach is better than the active based. In our work we are also using passive based approach and this is the most preferred approach to detect the digital image forgery for the past recent years.

The rest of the paper is organized as follows. In section II we discuss about the techniques which are available to detect the digital image forgery. Section III describes the method proposed by us to detect the tampered regions .section IV and V consists of results and conclusions respectively.

2 Digital Image Forgery Overview

As we discussed, the images are easily manipulated so it is advisable that we must not always believe that what we see is true. Here we are discussing the methods to detect tampered regions in the digital photo image. Xiaomei Quan et al [2] proposed a novel copy-move forgery detection scheme in digital images. It treats image as an high dimensional data and uses intrinsic dimension estimation to segment the image then detects the copy-move forgeries present in image region having same texture.

Xin Wang et al [3] put forward a passive blind digital image forgery detection based on consistency of defocus blur. Image patches which are at similar distance from lens have similar blur kernels and this consistency of blur is broken in the forged images which are used to detect the digital image forgery.

Fei Peng et al [4] proposed image forgery detection by using blur estimation and abnormal hue. Blurring is done to hide traces of forgery but it destroys the joint consistency of color channels in the image. Based on this

[a] Sarvjit Singh : sarvjit100878@yahoo.co.in

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

principle, blur estimation is done to the image and obtain the blur region, and exactly locate the artificial blur region by detecting the abnormal hue in the blur region.
Pravin kakar et al [5] proposed forgery detection by using in consistent motion blur. In order to find the spliced area in the digital image discontinuity in motion blur is used which in turn uses spectral matting for its estimation. In the end spliced area and remaining area are distinguished.
Jiri grim et al [6] uses local statistical models to detect the digital image forgeries. The local statistical models use Gaussian mixtures for the detection of tampered regions. This method detects the forgery of an image without any prior information.
Bo Xu et al [7] use phase correlation to expose image forgeries. This is a fast method which is based on non block matching based. If the image is forged then we get sharp peak in the phase correlation showing the proof of tampering.
Li kang et al [8] proposed a method to detect the copy move forgeries. But using block matching divide the whole image into equal blocks then to get a singular value matrix, singular value decomposition is applied to these blocks. In the end, the correlation coefficient is used to compare the blocks. Above are the methods of detecting digital image forgery and in the next section we are exposing digital image forgeries by Ant colony optimization (ACO).

3 Image Forgery Detection

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. In our paper, we are dealing with the copy-move forgery only. We have employed Ant colony optimization (ACO) methodology which is used to detect the copy-move forgery.

3.1 Introduction to ACO

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 [9].
As mentioned in [9], 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.

3.2 Proposed Methodology

The stepwise methodology is explained as follows:
Step 1: Firstly we 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. We take threshold value (50%).
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 =

$$\sum_{i=1}^{m}\sum_{j=1}^{m}(|I_i,j - K_i,j|)_R + \sum_{i=1}^{m}\sum_{j=1}^{m}(|I_i,j - K_i,j|)_G + \sum_{i=1}^{m}\sum_{j=1}^{m}(|I_i,j - K_i,j|)_B \quad \text{---------- (1)}$$

Where R, G and B denotes the subtraction for Red, Green and Blue matrices present in both current and ant block in equation (1).
And 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. For performance evaluation of the proposed method, we use two parameters namely Recall and precision rates. A brief description of which is given below:
The precision rate and recall rate are evaluated by using equation (2) and (3) respectively. Precision rate is defined as ratio of the parts detected correctly to summation of parts detected correctly and false positives. False positives are those regions which are actually authentic but detected as forged.

Precision rate

$$= \frac{\text{correctly detected parts}}{\text{correctly detected parts+false positives}} * 100 \quad \text{------- (2)}$$

Recall rate is defined as ratio of the parts detected correctly to the summation of parts detected correctly and false negatives. False negatives are those regions which are actually forged but detected as authentic.

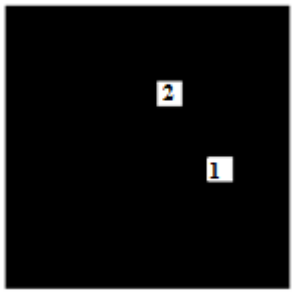
$$\textbf{Recall rate} = \frac{\text{correctly detected parts}}{\text{correctly detected parts+false negatives}} * 100$$

------- **(3)**

4 Experimental results

The experiments are performed in MATLAB and the format of images is JPEG. Our dataset consists of 50 images. In paper [10] JPEG compression technique and direction filter are used to detect the tampered regions in the digital photo image. In our work manipulation of images is done by using paint. We achieved better precision and recall rates than paper [10].

(a) Original image (b) Forged image



(c) Detected Forgery

Figure 1. Detection results of copy-move regions

The experimental results detecting the tampered regions are illustrated in following figures. Figure1 showing birds flying in the sky as a original image and copying one part of image containing bird and pasted on another part as forged image and in the last copy-moved parts are shown which we detect using ACO.
In our method, if there is any tampering in the original image then we obtain the black image of same size as that of original image showing high intensity on both the copy-moved parts as shown in figure1 and figure2.In the detected forgery the regions, shown in figure1(c) and figure2(c) which are labeled as **1** (of size 20X20) is the copied part in the image and the regions labeled as **2** is the pasted part (of size 20X20) showing high intensity at these regions.

(a) Original image

(b) Forged image

(c) Detected Forgery

Figure 2. Detection results of copy-move regions

In below table we are showing the performance comparison of method used in paper [10] and proposed method by using two parameters (precision rate and recall rate). These rates are calculated by using equations (2) and (3).

Table 1. Performance Comparison

Method Used	No. Of Images	Precision Rate	Recall Rate
Paper [10] (JPEG compression &direction filter based)	50	92.2	92.6
Proposed method (ACO based)	50	98.5	95.7

By using ACO, the precision rate is increased by 6.3% and recall rate is increased by 3.1% than the method used in paper [10]. It means ACO gives better performance than the method used in paper [10].

5 Conclusions

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 we have mentioned the intelligence technique (ACO) in our paper. Our method has given satisfactory experimental results. The proposed method shows excellent detection of the tampered regions. The advantage of our approach is to find the manipulated areas present within the input image precisely and accurately. Our proposed algorithm promises to expose the digital image forgery created by copy-move method.

6 Future Scope

In today's digital world, a lot of work has been done for the detection of digital image forgery. But there is a still scope of future work so that the image forgery can be detected more accurately and precisely.
Although in the proposed work, recall rates and precision rates have been increased but they can be further improved. As the precision rate and recall rate depends on false positives and false negatives respectively. So, the reduction of false positives and false negatives in future will give more improved results. Hence, it will help in achieving the ultimate goal i.e. accurate detection of image forgery.

References

1. S.Khan, A. Kulkarni, "*An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform*," IJCSE, **2**, No.5, pp: 1801-1806, (2010)
2. X. Quan, H.B. Zhang, "*Copy-Move Forgery Detection in Digital Images Based on Local Dimension Estimation*," IEEE ICCSCWDF International Conference on (CyberSec), pp: 180 – 185, (2012)
3. X. Wang, B. Xuan, S. L. Peng, "*Digital image forgery detection based on the consistency of defocus blur*," IEEE ICIIHMSP, pp: 192 – 195, (2008)
4. F. Peng, X.L.Wang, "*Digital image forgery forensics by using blur estimation and abnormal hue detection*," SOPO, pp: 1 – 4, (2010)
5. P. Kakar, S. Natarajan and W. Ser, "*Detecting Digital Image Forgeries through Inconsistent Motion Blur*," ICME, pp: 486 - 491, (2010)
6. J. Grim and P. Somol, "*Digital Image Forgery Detection by Local Statistical Models*," IIH-MSP), pp: 579- 582, (2010)
7. B. Xu, G. Liu and Y. Dai, "*A Fast Image Copy-move Forgery Detection method using Phase Correlation*," MINES, pp: 319-322, (2012)
8. L. Kang and X. Cheng, "*Copy-move Forgery Detection in Digital Image*," CISP, pp: 2419-2421, (2010)
9. Chandrasekhar, N.P.Rao, "*Recent trends in Ant Colony Optimization and data clustering: a brief survey*," IAMA, pp: 32 – 36, (2011)
10. S. Murali, B. S Anami, G. B Chittapur., "*Detection of Digital Photo Image Forgery*," IEEE -ICACCCT, pp: 120 – 124, (2012)