International Journal of Imaging Science and Pattern Recognition
Volume 1 Issue 1

Efficient Detection Technique for Image Forgery

V.Suresh
Assistant Professor/CSE
Dr.N.G.P.Institute of Technology

T.Primya
Assistant Professor/CSE
Dr.N.G.P.Institute of Technology

G.Kanagaraj
Assistant Professor/CSE
Kumaraguru College of Technology

Abstract

Image forgery is a real time issue in this present era and causes a lot of tribulations to the society. The forgery in an image includes object addition, object removal, changing color etc. The overture of our work is to find the type of forgery present in an image i.e. whether the image is retouched or copy move forgery. While comparing to copy move forgery, Retouching is not a major kind of forgery because it is used only for clarification purpose and also in this paper we are going to propose a fuzzy logic algorithm for segmentation of an image to improve the accuracy rate of detecting the cloned region in an image. Initially the image was segmented into patches and a keypoint was extracted in each patches. The detection of cloned region is done in two stages. In first stage, an affine transform matrix was built by finding the suspicious pairs in an image. In second stage, the detection of cloned region can be accurately detected using Fuzzy technique.

Keywords: *Forgery, copy move, retouching, cloned region, fuzzy logic, affine transform matrix, CMF*

INTRODUCTION

Now A Days the use of images is increasing day by day. And there is a lot of image editing software which makes forgery in an image easily. There are mainly three types of forgery present in an image.

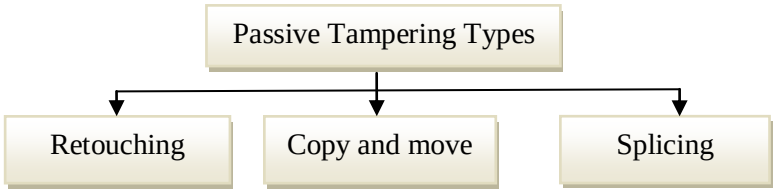

Fig 1.1 *Types of Passive Tampering*

Comparing to CMF (Copy Move Forgery) and Splicing, Retouching is not a major kind of forgery [1]. Image Retouching is not a major kind of forgery [4]. Image Retouching only try to enhance some of the feature of an image. This technique is famous in Image Advertisement, Newspapers in order to improve the clarity of an image. So Retouching only modifies the color of the picture and does not modify any other features present in an image .

Fig 1.2 *Photo captured in NASA*

Image Splicing is more aggressive than image retouching [4]. Image Splicing is a technique that involves a composite of two

or more images which are combined to create a fake image [1].

Fig 1.3 *Example of Image Splicing*

Copy-move attack is more or less similar to Image Splicing in view of the reality that both techniques modify certain image region with another image [1]. Instead of having an external image as the source image, copy-move attack utilize portion of the original image as its basis. In other words, the source and the destination of the modified image originated from the same image [7]. In a copy-move attack, parts of the original image is copied, moved to a desired location and pasted this is usually done in order to conceal certain details or to duplicate certain aspects of an image. Blurring is usually applied along the border of the modified region to reduce the effect of irregularities between the original and pasted region [1].

Fig 1.4 *Example of copy-move attack*

II.LITERATURE REVIEW

To find copies present in the same image SIFT based approach is used. The SIFT based approach consists of three parts: Cluster the Key points, Matching patches, Texture analysis [2]. In SIFT Matching Patches, the extracted points are compared with other points of the same image if the points contain the similarity when it copied form one region to another region. To improve the detecting and finding the copy and move present in the image objects are compared between them. The SIFT points are extracted from the image and the similar points are grouped using the technique agglomerative hierarchical-tree cluster method [2]. Cluster tree formed for comparing the points of the object with other object. The matching points are counted for each comparison if the counted value is high then the cluster is taken into the account for further process. For improve the efficiency in case of multiple maxima the lowest number of clusters are selected. To eliminate the false matches the texture descriptors are used. Tampering detection techniques contain two approaches Blind and Non-blind [7] .The Blind approach requires the original image for the forgery detection but the Non-blind approach does not require the original image for detecting the forgery present in an image. Segmentation used separating the image based on feature present in the image. Different types of segmentations are available for separate the image [3]. The Segmentation Types are: Threshold based, Edge based, Region based, Clustering Technique, Matching. In Threshold based Segmentation the Histogram thresholding and slicing techniques are used to segment the image [4] [5]. Edge based segmentation. With this technique, detected edges in an image are assumed to represent object boundaries, and used to identify these objects. A region based technique takes the opposite approach, by starting in the middle of an object and then “growing” outward until it meets the object boundaries. Clustering technique goal is very similar to what we are attempting to do when we segment an image, and indeed some clustering techniques can readily be applied for image segmentation [3]. When we know what an object we wish to identify in an image (approximately) looks like, we can use this knowledge to locate

the object in an image. This approach to segmentation is called matching.

PROPOSED SYSTEM

In this paper, we are going to predict the type of forgery present in an image. The reason for predicting the forgery type is to prioritize the forgery in an image. Comparing to copy-move forgery and splicing, Retouching is not a major kind of forgery because it is used for clarification purpose [1]. And also in this paper we were going to propose an efficient algorithm to detect the cloned region in the image. An image with CMF contains atleast a portion are identical. There are two classes of CMFD algorithm [2]. One is based on block-wise division and the other on keypoint extraction [3]. In this paper, an efficient technique called Fuzzy logics K-Means clustering algorithm [6] was used to accurately detect the cloned region in an image.

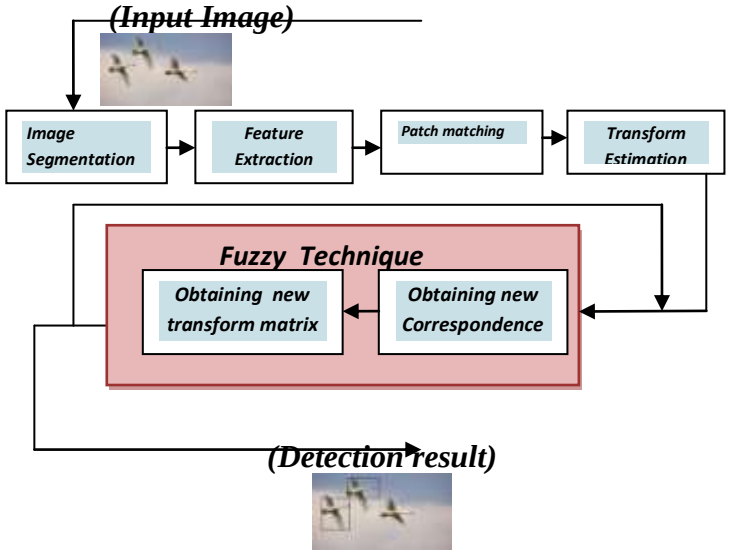

***Fig 2.1** Architecture diagram for Proposed system*

Input Image

It is the first step in forgery detection and an image that may be with or without forgery is given as input.

Image Segmentation

In order to distinguish the copied region from the original region, the image must be segmented into number of patches. The patches are divided according to the similarities present in the pixel. And the CMF region may not be present in the same patch.

Keypoint Extraction and Description

In order to extract the keypoint vlFeat software was used [3]. In order to obtain convicting result maximum keypoints must be extracted.

Patch Matching

In case of original image, the frequency present in an image increases periodically. But by copying and pasting one region into another then there is a drastic change in frequency at that point [3]. So by comparing with these keypoint, an affine transform matrix is constructed. In block-based algorithm, it only focus on finding the tampering regions and do not consider about the transform relationship between the copying region and the target region [3].

Fuzzy Technique

In order to improve the accuracy rate of detecting the cloned region an efficient technique, Fuzzy K-means algorithm is used [6]. The main advantage of using fuzzy technique is that performs the keypoint comparison repeatedly so that the accuracy rate gets improved.

PROPOSED SYSTEM-FUZZY K-MEANS ALGORITHM

To classify or to group the object based on the feature present on the image. The grouping is done by minimizing the sum of squares of distances between data and the corresponding cluster centroid. Thus, the purpose of K-mean clustering is to classify the data [6]. If the number of data is less than the number of cluster then we assign each data as the centroid of the cluster. Each centroid will have a cluster number. If the number of data is bigger than the number of cluster, for each data, we calculate the distance to all centroid and get the minimum distance. This data is said belong to the cluster that has minimum distance from this data. Since we are not sure about the location of the centroid, we need to adjust the centroid location based on the current updated data. Then we assign all the data to this new centroid. This process is repeated until no data is moving to another cluster anymore.

STEPS

Let X={x1,x2,x3,…xn} be the set of data points and V={v1,v2,..vc} be the set of centers.

Algorithm

1. Select ‘c’ cluster centers.
2. Find distance between each data point and cluster centers.
3. Assign the data point to cluster center whose distance from the cluster center is minimum of all the cluster centers.
4. Recalculate the new cluster
5. Recalculate the distance between each data point and new obtained cluster centers.

6. If no data point was reassigned then stop, otherwise repeat from step 3.

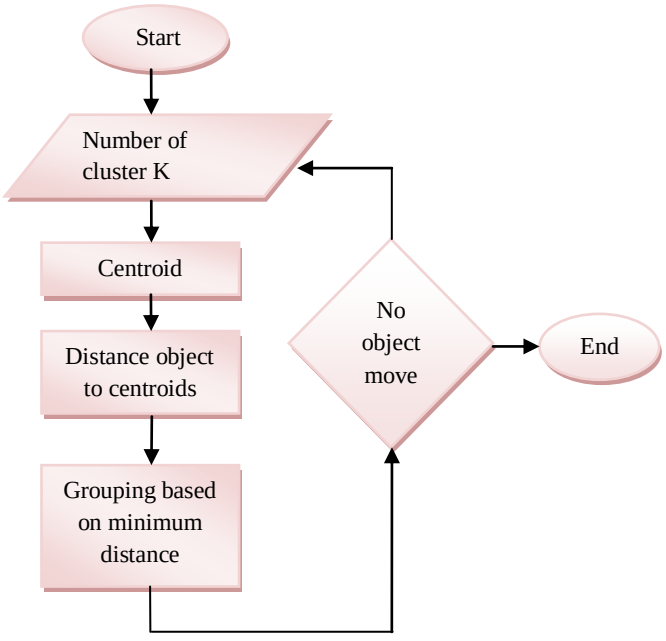

Fig 2.1 *Flowchart for calculating new cluster*

EXPERIMENTS AND RESULTS

Global contrast enhancement detection algorithm:

Pre-processing

In pre-processing, we convert color image into gray image and apply histogram equalization on the converted image. Here we are applying histogram equalization [5] as a form of contrast enhancement in order to create a contrast enhanced image.

Fig 5.1 *Original Color image is converted to gray level Image and then the image is contrast enhanced*

Histogram Calculation & zero bin count:

The input image is then used in histogram calculation and histogram of the image [5] is calculated. Zero-bins are calculated from the histogram of the image. Zero bins are the bins whose value is found to be null [4] .

Min & Max Pixel Value calculation:

In Min & Max pixel value calculation, we calculate the minimum and maximum pixel value of the image.

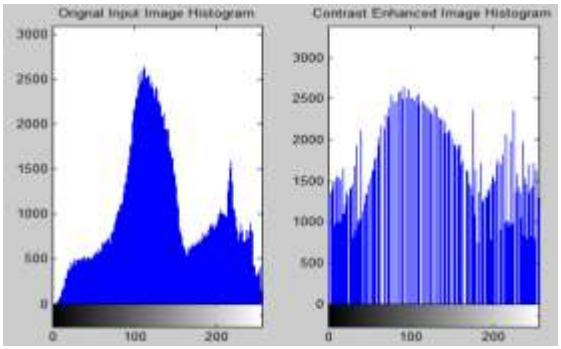

Fig 5.2 *Shows the Histogram of Original Color image and the Histogram of Contrast enhanced Image*

Forgery Detection:

After getting the zero-bin count and minimum & maximum pixel value of the image [4], we apply the threshold condition. Threshold condition can be given as:

Threshold = zero count >18 && max > 248 && min < 10

If this condition is satisfied, contrast enhancement is said to be detected otherwise, no contrast enhancement is said to be done.

CONCLUSION

This paper proposed a Fuzzy techniques k-means algorithm to improve the accuracy rate in the cloned region. And also the type involved in the forgery was also detected. Our contributions are proposed a Fuzzy technique to improve the accuracy rate of detecting the cloned region and predicted the type of forgery involved in the image i.e. retouching or copy-move forgery.

FUTURE ENHANCEMENT

The proposed system detects the kind of forgery present in the digital image. Only copy move forgery and retouched images can be predicted using the proposed method so we try to detect spliced images in the future work.

REFERENCES

1. 1. Snigdha K.Mankar, Dr.Ajay A.Gurjar, “Image Forgery Types and their detection: A Review” In International Journal of Advanced Research In Computer Science and Software Engineering April 2015.
2. E.Ardizzone, A.Bruno, G.Mazzola, “Detecting Multiple copies in Tampered Images” In IEEE 17th International conference on Image Processing September 2010.
3. Jian Li, Xiaolong Li, Bin Yang, Xingming sun, “Segmentation-Based Image Copy-Move Forgery Detection Scheme” In IEEE Transactions on

Information Forensics and security March 2015.
4. Mahesh Mahipati Patil, S.P.Rangdale, S.A.Nalawade, "Digital Image Alteration Detection using advanced Processing" In International Journal Computer Applications April 2015.
5. Jayshri Charpe, Antara Bhattacharya, "Detecting Image forgery using Intrinsic Fingerprints" In International Journal of Advance Research in Computer Science and Management Studies June 2015.
6. Weiling Cai,Songcan Chen,Daoqiang Zhang, "Fast and Robust Fuzzy C-Means Clustering Algorithms Incorporating Local Information for Image Segmentation"
7. Minati Mishra, Dr. M.C. Adhikary "Digital Image Tamper Detection Techniques-A comprehensive Study" In International Journal of Computer Science and Business Informatics June 2013.