Survey On Fraud Image Detection

Miss. Rutuja Jadhav
Student
Marathwada Mitra Mandal's College of Engineering
Pune, India

Miss. Sneha Chavan
Student
Marathwada Mitra Mandal's College of Engineering
Pune, India

Miss. Khushboo Patil
Student
Marathwada Mitra Mandal's College of Engineering
Pune, India

Miss. Snehal Shivankar
Student
Marathwada Mitra Mandal's College of Engineering
Pune, India

Mr. Mukesh More
Professor
Marathwada Mitra Mandal's College of Engineering
Pune, India

***Abstract*—Image Forgery means manipulation of digital image to conceal meaningful information of the image. The detection of forged image is driven by need of authenticity and to maintain integrity of an image. A copy move forgery detection theme victimization, adaptive over segmentation and has purpose feature matching is used. Earlier block based forgery detection is used but this algorithm has some flaws like: the host image is divided in to overlapping rectangular blocks, which would be computationally expensive, as size of the image increases. The method cannot address the significant geometrical transformations of the forgery regions and their recall rate is low because image blocking method is of regular shape. Although this method can avoid above two problems reducing the computational complexity thus successfully detect the forgery. This method integrates both traditional blocked base forgery detection method and key-point based forgery detection method.**

We use an image blocking method called as adaptive over segmentation algorithm to divide host image into non-overlapping and irregular blocks adaptively, the feature points are extracted from each image block as block feature instead of being extracted from the whole host image. We use SLIC (simple linear iterative clustering) to segment the host image into meaningful irregular super pixels. To analyze the frequency distribution of the host image DWT (Discrete wavelength transform) is used to describe the local features in image SIFT (Scale Invariant feature transform) is being used. Another method that we are using for exposing cut-paste based image forgery, contrast enhancement detection technique is adapted. To detect contrast enhancement in an image histogram based detection is applied.

***Keywords*— SLIC, DWT, SIFT, Histogram, Equalization.**

I. INTRODUCTION

In this aeon, digital image forgery has been increasing tremendously, so the reliability of the image thus becoming vital issue to be focused on. By using open source tools like Adobe Photoshop, GIMP, Coral Paint fake image can be created There are many cases in digital image forgery, which are classified into three categories based on process of creating fake images like image retouching, image slicing, copy-move attack. Cut- paste forgery detection is carried out by histogram equalization technique. Histogram equalization is a technique use for adjusting image intensities to enhance contrast. Histogram equalization is basically equal to pixel value mapping, which shows some statistical traces. According to the contrast detection graph shows sudden change in the peak levels. It achieves great result for detecting the forgery intensities can be better distributed on the histogram.

II. EXISTING SYSTEM

In earlier block based forgery detection was used to detect forged image but this algorithm faced some drawback such as the host image is divided into overlapping rectangular blocks, which would be computationally expensive as the size of image increases and it was less efficient. Disadvantages It takes more time to process due to over-lapping rectangular blocks.

III. COPY-MOVE TECHNIQUE

Along with block based forgery we use an image-blocking method called adaptive over-segmentation method that divide the host image into non overlapping blocks adaptively with the help of two algorithms those are Simple Linear Iterative Clustering (SLIC) to segment the host image into irregular blocks and Discrete Wavelength Transform (DWT) which is employed to analyze the frequencies of the super pixel. Further the image block form are passed to the block feature extraction method where the block feature are extracted by using Scale Invariant Feature Transform (SIFT) as it possess constant and better performance compared with other extraction method. Further the process of block feature matching is carried out which uses simple linear iterative clustering for calculating super pixels and discrete wavelength transform are finding super pixel from one block and checking other pixels from other blocks. When the features are extracted and matched then

we get to know which regions the host image has been forged as shown in Fig. 1.

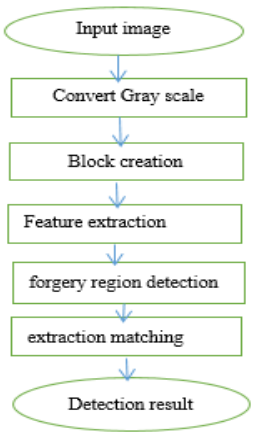

Fig. 1. Flowchart of copy-move technique.

IV. ALGORITHMS FOR COPY-MOVE DETECTION TECHNIQUE

A. Adaptive Over-Segmentation

The Adaptive Over-segmentation method can segment the host image into non-overlapping regions of irregular shape as image blocks the forgery regions then can be detected by matching those non-overlapping and irregular regions. We use the simple linear iterative clustering (SLIC) algorithm to segment the host image into meaningful irregular super pixels, as individual blocks. The SLIC algorithm adapts a k-means clustering approach to efficiently generate the super pixels and it adheres to the boundaries very well. SLIC algorithm is computationally less expensive than that of the traditional adaptive over segmentation algorithm.

ALGORITHM 1

INPUT: Host Image.

OUTPUT: Image Blocks.

STEP1: Calculate the super pixel by using K-means clustering method.

STEP2: Calculate high level and low level of frequency by using DWT algorithm.

STEP3: Obtained irregular blocks

STEP1: Super pixel is a feature point that contains maximum point and adheres in the boundary as well. If value of super pixel is smaller it results into expensive computation and if it has large value then result is not accurate. Therefore the accurate value of the super pixel is vital. Initial size of the super pixels adaptively based on the texture of the host image. Smoother the image size of super pixel is set to relatively large and detailed the image size of super pixel is relatively small.

STEP2: To determine this frequency of an image DWT algorithm is used (Discrete Wavelet Transform).Using ”HAAR wavelet” calculate high level frequency and low level frequency.

STEP3: We obtained image in irregular blocks

B. Matching Of Block Feature

In this section, extraction of block features from the image blocks is obtained. Among all the feature points’ extraction methods SIFT and SURF has been widely used in the field of computer Technology. SIFT stands for scale-invariant feature transfer and SURF stands for Speeded up Robust Features. The SIFT has constant and better performance compared with the other image feature extraction method. Therefore in this paper, we are detecting fraud image using SIFT algorithm.

In this method one can also change the scale, rotation, illumination and viewpoint, and still get good results. Using a stage filtering approach scale-invariant can be identified easily.

ALGORITHM 2

INPUT: Image with irregular blocks

OUTPUT: labeled feature points

STEP1: Construct scale space and obtain octaves by using

$L(x,y,\sigma)=G(x,y,\sigma)*I(x,y)$.

STEP2: Carry out LoG approximations.

STEP3: Getting key point localization i.e finding key points D(x) = D+x

STEP4: Elimination of low contrast key point

STEP5: key-point orientation is carried out where point is to be checked for suitable cluster.

STEP6: Retrieval of features.

STEP 1: In first stage includes construction of scale space. In this, internal representation of the original image is created to ensure a scale invariance. Several octaves of the original image is generated where each octave's image size is half of the previous one. In this octave, images are progressively blurred using the Gaussian Blur operator. It had been suggested that four octaves and five blur levels are ideal for the algorithm the creator of SIFT.

STEP 2: In second stage includes Difference of Gaussian (DoG) which is an approximation of LoG. In this stage two successive images in an octave are selected and one is subtracted from the other. Then the next successive pair is taken, and the process repeats. This is done for all octaves.

STEP 3: Third stage is key localization. This technique detected the maxima and minima in the DoG images generated in the above stage. This is done by comparing adjacent pixels in the current scale, the scale "above" and the scale "below”. Using the available pixel data, sub-pixel values are generated. This is done by using the Taylor expansion method. Mathematically, it's like this: D(x) = D+x +

STEP 4: fourth stage is elimination of bad key points. Potential key point locations have to be refined to get more accurate results, once they are found.

STEP 5: In fifth stage an orientation is assigned to each key point to achieve invariance to image rotation. An adjacent is taken around key point location depending on the scale, and the gradient magnitude and direction is calculated in that region.

STEP 6: In final stage a 16x16 window of "in-between" pixels around the key point is taken. We split that window into sixteen 4x4 windows. From each 4x4 window you generate a histogram of 8 bins. Each bin corresponding to 0-44 degrees, 45-89 degrees, etc. Gradient orientations from the 4x4 are put into these bins. This is done for all 4x4 blocks. Finally, we get normalized 128 values.

C. Forgery Region Extraction

ALGORITHM 3

INPUT: Labeled feature points.

OUTPUT: Detected forgery region.

STEP1: Application of SLIC and find subpixels.

STEP2: Measure super pixels of sub blocks and merge them.

STEP3: Apply morphological operation and generate forgery region.

V. CUT-PASTE IMAGE FORGERY DETECTION TECHNIQUE

A. Histogram Equalization

By the immediate development in the field of editing in digital image, image manipulation becomes very easy. Sometimes it is legal and beneficial and sometimes it is suspicious. Some application such as crime related situations it is necessary to detect any suspicious activity will be happened and the history of that image. For verifying these, digital image forensic technique have been used. Some forensic methods detects whether manipulation occurred or not but fails to detect which specific type of activity is done. Another category of forensic techniques detect specific image manipulations. In contrast enhancement forensic algorithm performs well under the assumption that the gray level histogram of an unchanged image exhibits a smooth curves. Gray level histogram of unaltered images shows smoothness while that of contrast enhanced images shows peak artifacts. Using histogram equalization we can easily detect whether image forged or not. An important application is to identify cut-and-paste type of suspected images, in which the contrast of one source region is shifted to match the next. In both-source enhanced composite forged image. The two source images used for creating cut-and-paste type of forged images may have different color temperature or luminance contrast. So, in order to make the forged image more real, contrast enhancement is performed on either one or both the regions. However, cut-and-paste type of images created by enhancing single source could be identified in prior work, but it fails to detect the both source-enhanced cut-and-paste type of forged images. Contrast enhancement is use to give finishing to the cut-paste image, so that it would not be able to recognize by naked eyes. Histogram equalization is based on two concepts: 1) PMF (probability mass function) 2) CDF (cumulative distributive function).

Flowchart of cut-paste technique is given below:

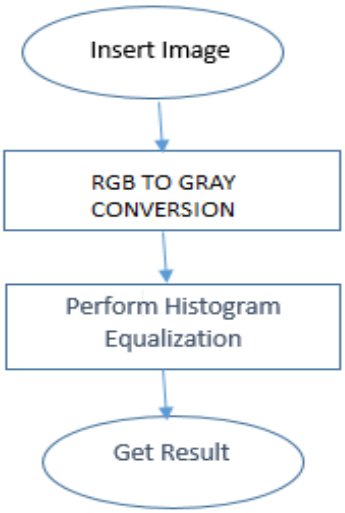

Fig. 2. Cut-paste flowchart.

ALGORITHM 4

STEP1: Insert host image.

STEP2: Perform histogram equalization.

STEP3: Calculate PMF and CDF.

STEP4: Graph will be plotted.

STEP5: Detected image forged or not.

We can detect whether image is cut-paste or not is determine by observing histogram.

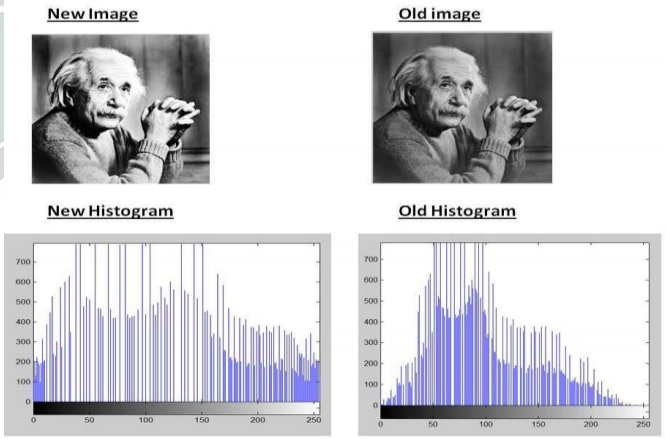

Fig. 3. Histogram Equalization.

As you can clearly see from the images that the new image contrast has been enhanced and its histogram has also been equalized. There is also one important thing to be note here that during histogram equalization the overall shape of the histogram changes, where as in histogram stretching the overall shape of histogram remains same.

CONCLUSION

By using adaptive over segmentation and feature point matching algorithm for image forgery we have overcome with

the major problem of overlapping and time complexity. The applied algorithms results in very efficiently in terms of processing and time consumption and using histogram equalization technique Gray level histogram of unaltered images shows smoothness while that of contrast enhanced images shows peak artifacts. Using histogram equalization we can easily detect whether image forged or not.

REFERENCES

[1] Aditya R Hambarde and Avinash G Keskar,"Copy-move forgery detection using DWT and SIFT features", proceeding Department of Electronics Engineering Visvesvaraya National Institute of Technology, Nagpur, India 'farooq78699 .

[2] Mr.Arun Anup M,"Image forgery And Its Detection: A survey (2015)",Department of computer engg and science, MES college of Engineering.

[3] Vincent Christlein," An evaluation Of Popular Copy-Move Forgery Detection Approaches", Student member IEEE,vol.07.no 6 December 2012

[4] X.bo.w.Junwen," Image Copy-Move forgery detection based on SURF" , in proc. Int. conf., multimedia inf. Netw.(MINES). Nov .2010.

[5] Jessica Fridich and David Soukal,"Detection Of Copy Move Forgery In Digital Image", Department of computer Science, NY 13902-6000.

[6] [20] D. G. Lowe, "Object recognition from local scale-invariant features," inProc. 7th IEEE Int. Conf. Comput.

[7] 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.

[8] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding. Berlin, Germany: Springer-Verlag, 2010, pp. 51–65.

[9] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulos, "An evaluation of popular copy–move forgery detection approaches," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[10] Chi-Man Pun, Xiao-Chen Yuan," Image Forgery DetectionUsing AdaptiveOversegmentation and Feature Point Matching" Senior Member, IEEE.