"Digital Image Forgery Detection using SIFT Feature"

Bhavesh Patil
B.E. Student of Computer Engineering
Atharva College of Engineering, Mumbai University
Mumbai, MH, India

Sayali Wade
B.E. Student of Computer Engineering
Atharva College of Engineering, Mumbai University
Mumbai, MH, India

Akshata shivade
B.E. Student of Computer Engineering
Atharva College of Engineering, Mumbai University
Mumbai, MH, India

Amruta Sankhe
Prof. of Computer Engneering
Atharva Collage of Engineering, Mumbai University
Mumbai, MH, India

***Abstract*- Availability of new software's nowadays, one can create unauthentic images quite often. Mostly used media to create unauthentic images for public sizing false reports. Also, in crime one can make changes in an image using various attacks such as copy-move attack, tampered and composite. For solving these problems of image forgery various detection methods are to be used and then compared, in order to specify which method is more beneficial to be used in a particular type of attack.**

To detect such modifications, a novel methodology based on SIFT: Scale Invariant Feature Transform is proposed with feature extraction which is invariant to translation, scale, noise and rotation. It comprises transformation of the input image to produce a standard results and then detection of keypoint and feature descriptor is applied along with a matching over all the keypoints. It comprises of the input image to produce standard representation and detection of duplicate image.

1. INTRODUCTION

Nowadays lots of sophisticated digital cameras and powerful photo editing software tools are easily available.it has become very easy to alter the digital images and create forge image which are difficult to distinguish from forged image and authentic digital image. With the development of advance technology and freely available software like adobe Photoshop and CorelDraw it become very easy to tempered the image or create manipulated image without leaving any clue.an image can be tempered in various ways such as deleting some part of the image, hide some part of image, cut some part and paste it on unwanted part of the digital image, adding new part in the image, etc. our project helps to detect tempered image or manipulation done in the digital image. For such type of detection we are going to Scale Invariant Feature Transform (SIFT) algorithm[1]. Scale Invariant Feature Transform is an algorithm in a computer vision to detect and describe local feature in the digital image. This algorithm was published by David Lowe 1999. SIFT's application include object recognition, robotic mapping and navigation, image stitching, 3D modelling, gesture recognition, video tracking[1].

2. REVIEW OF LITERATURE

The meaning of tampering is interfering with something so as to make unauthorized alterations or damages to image. Image tampering can be performed either by making changes to the context of the scene elements or without the change of context. Digital image tamper detection techniques are classified into two techniques – active detection technique and passive detection technique. There are two techniques popularly used passive detection techniques splicing and cloning[2].

Copy move attack in which part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. A copy move forgery introduces a correlation between original image and pasted one. This correlation can be used as a basis for successful detection of this type of forgery. Because the forgery will likely be saved in the loss JPEG format and because of possible use of the retouch tool or other localized image processing tools, the segment may not match exactly but only approximately[4].

A method for detecting copy-move forgery which is one of the difficult types of forgery. This method is good at some manipulation like JPEG compression, rotation, Gaussian noise, smoothing, scaling etc. The image is partitioned into blocks and exact matches are made between patterns of different blocks and then results are calculated using Discrete Wavelet Transform[5].

A detection method is proposed to effectively locate image forgeries by detecting inconsistency of image noise variance on the saturation component of HSV colour space. The image is first converted to HSV colour space from RGB colour space. Then images were divided into small blocks of different sizes and 100 forged images were randomly cropped at different locations from the images for each size and white Gaussian noise was added. The evaluations results describe that the noise estimation for image blocks with size of 32×32 achieved the best results. However the drawback was that the noise estimation for 16x16 and 64x64 pixels images was poor[6].

A method for tampering detection in which the original image is divided into overlapped blocks and for each block number of connected components are calculated. By calculating the difference between vectors of the original image and tampered image the location of tampering is detected and measured. However the drawback of this method is that it is applicable on similar sized square images only. In future it can be extended to different sized images[8].

A composite image is created by taking a particular region from a source image and pasting it into a target image after performing geometric operations. The composite image contains tampered and untampered regions. Feature inconsistency is used for the tampering detection, such as feature inconsistency based on noise, JPEG compression, and shadows[9].

The SIFT keypoints described in this; it enables the correct math for keypoint to be selected from large database of other keypoint. It transforms image data into scale invariant coordinates relatives to local features. In keypoint localization, once a keypoint candidate has been found by comparing a pixel to its neighbours, next step is to perform detailed fit to the nearby data for location, scale and ratio principle[7].

3. EXISTING SYSTEM

For detection of manipulated image there are many detection techniques were already introduced in past literature. But those techniques are not able to handle the rotation and scaling transformation. These techniques can detect only copy move type of forgery done in the digital image. But SIFT techniques are invariant to translation, scale, noise and rotation and SIFT techniques can also detect all type of manipulated image i.e. copy move image, tempered image, composite image.
Previous detection techniques are mention below:-

1. Segmentation-Based Image Copy Move Forgery Detection Scheme[10]

- This technique is two stage processes.
  Stage 1: Find the suspicious matches along with rough transform matrix.
  Stage 2: confirm the existence of CMF by refining the transform matrix.
- It uses keypoint matching mechanism.
- It can detect forged regions of size as small as 32*32.
- Detection speed is slow.

2. Improved SIFT-based Copy-move Detection Using BFSN Clustering and CFA Features[10]

- This technique combines SIFT with Broad First Search Neighbours (BFSN) and Color Filter Array (CFA) features.
- It uses cluster matching mechanism.
- Advantage:
  - Detect multiple copied regions and discriminates original and forged region.
- Disadvantage:
  - Flat CMFD regions not detected.

3. Copy-Move Image Forgery Detection Based On Sift Descriptors And Svd-Matching[8]

- It uses SIFT vectors used to compute correlation vector proximity matrix and similarity matrix. Matching points thus calculated then subjected to a fusion step.
- This technique uses keypoint matching mechanism.
- Advantage:
  - Automatic method to detect duplication in image region.
- Disadvantage:
  - Reduced the number of false point matching problem.

4. Speeding up SIFT based copy move forgery detection using level set approach[9]

- In this technique image is segmented using chan-vese segmentation method. Keypoints in ROI are matched and copy moved region detected.
- This technique also uses keypoint matching mechanism.
- Advantage:
  - Multiple-forged object detection.
  - Robust and simple implementation.
- Disadvantages:
  - Usage of boundary properties alone and not including the regional properties.
  - Fixing the threshold for the matching process.

5. Detection of copy forgery in digital images based on LPP[9]

- It uses SIFT with Locality Preserving Projections (LPP). LPP used to obtain reduced dimensional feature descriptors.
- Keypoint matching mechanism is used in this technique.
- Advantages:
  - Uses dimension reduction method
  - Speed up the process of CMF detection.
- Disadvantages:
  - Not effective in images with forged regions with small area and on flat surface.

6. Fast and robust passive copy-move forgery detection using SURF and SIFT iamge features[7]

- It is two stage processes. It merges the SIFT method along with SURF techniques and use the G2NN method to detect the similar feature matching technique.
- It also uses keypoint matching mechanism.
- Advantage:
  - Fusing two feature detection method increases the efficiency and robustness of CMF detection.

- Disadvantage:
  - Number of keypoints affect processing time
  - Cannot detect multiple cloned regions and a patches with uniform texture is missed.

7. Copy move forgery detection using DWT and SIFT feature[8]

- It uses DWT method for dimensionality reduction. SIFT features extracted from the LL part of the DWT analysed image.
- Keypoint matching mechanism is also used in this technique.
- Advantages:
  - High accuracy as compared to other method
  - Reduced computation complexity.
- Disadvantages:
  - Block based method efficiency affected by image size.

8. SIFT based forensic method for copy move attack detection and transformation[10] recovery

- It consists of SIFT feature extraction, similar feature matching, hierarchical clustering, geometric transformation. It uses iterative generalized 2NN test to find similar keypoints and agglomerative hierarchical clustering performed on similar points.
- It uses both cluster and keypoint matching mechanism.
- Advantages:
  - Can detect multiple copies of cline region.
- Disadvantages:
  - Cannot detect copied image patch having maximum uniform texture such as the salient keypoints that are not covered by SIFT.

9. Region duplication detection using image feature matching[9]

- In this initially the keypoints are collected and then rough keypoint matching is done. Then finding of affine transform between matched keypoints. Finally region correlation map generated for locating duplicate regions.
- This technique also uses keypoint matching mechanism.
- Advantages:
  - It can detect multiple copied regions.
- Disadvantages:
  - Cannot detect region with little visual structure.

10. Detecting multiple copies in tampered image[10]

- This method search for objects that match and fully automatic. It is three step approach SIFT keypoint clustering, similar cluster matching and texture based analysis.
- This technique uses cluster matching mechanism.
- Advantages:
  - Robust upto jpeg compression level of 30.
  - Texture analysis is utilized to differentiate the matching.
  - Robust to false matches.
- Disadvantages:
  - Setting higher value, clusters results in too few points.
  - That may not be enough to find matches that may claim similarity between the detected points.

4. PROPOSED SYSTEM

Our proposed system used to detect the alteration or manipulation done in the digital image with the help of SIFT feature. The detection process is as follows:

Process

- Suspected images are scanned and processed. Various conversions take place.
- Then starting and ending pixels are correlated.
- The pixels are selected and highlighted. Those finally selected pixels are the key points for further processing.
- After selecting the keypoints scale space is constructed and for this we are going to use Gaussian filter and hessian matrix.
- Select the areas of the object detected in the image.
- We match the objects with equal areas. Techniques are used to tally the other features of the object.
- Two expected results could appear

- In case, if the object gets matched then further analysis is done.
- In case, if the object does not match, then we consider that the image is authentic only.
- The image with the objects having same area is notified.
- Show the objects having forgery in them.

5. METHODOLOGY

The overall method of our proposed system as shown in the following fig. 1

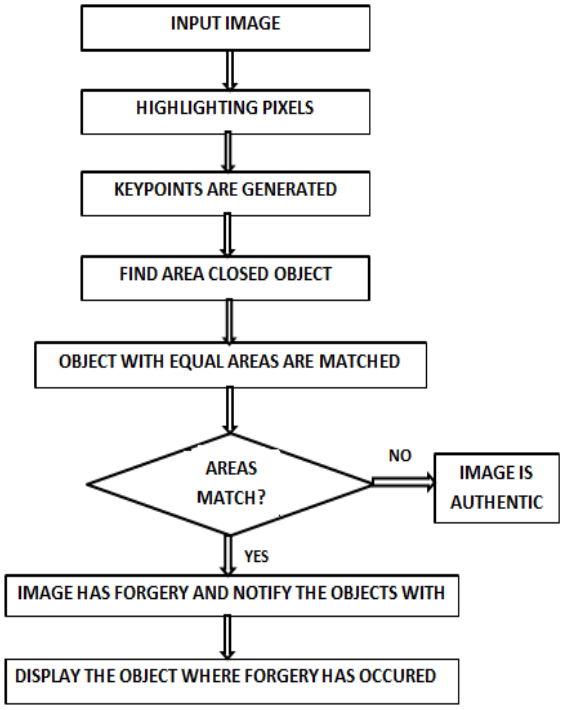

Fig. 1 Methodology

In our proposed system forged image is detected by following steps:

Step 1- Input

Suspected images are scanned and processed. Various conversions take place.

Step 2- Highlighted pixels (any closed pixel)

Here the starting and ending pixel are co-related.

Step 3- Keypoints generated

The pixels are selected and highlighted. Those finally selected pixels are the keypoints for further processing.

Step 4- Find areas of object

Select the area of object detected in the image.

Step 5- Objects with equal areas are matched

We match the areas with equal areas. Techniques are to tally the other features of the object.

Step 6- Condition (If the area gets matched)

Two expected result could appear:

In case, if the object gets matched then further analysis is done.

In case, if the object does not match, then we consider that the image authentic only.

Step 7- Notify the object having forgery

The image with the object having same areas is notified.

Step 8- Display the forged object

Show the objects having forgery in them.. .

CONCLUSION

Scale Invariant Feature Transform (SIFT) algorithm is used for this project. Scale Invariant Feature Transform is an algorithm in a computer vision to detect and describe the local feature in the digital image. SIFT algorithm is invariant to scaling, noise and rotation transformation. This system is commonly used for detection of the manipulation done in the digital image (image forgery).

REFERENCES

[1] Rajeev Rajkumar; Kh. Manglem Singh "Digital image forgery detection using SIFT feature" Advanced Computing and Communication (ISACC), 2015 International Symposium on
[2] Neetu Yadav and Rupal Kapdi Copy Move Forgery Detection Using SIFT Features- An Analysis
[3] A Langille and M. Gong, "An efficient match-based duplication detection algorithm", IEEE CRV, p. 64, 2006.
[4] J. Fridrich, D. Soukal and 1. Lukas, "Detection of copy-move forgery in digital images", Proc. IEEE Digital Forensic Research Workshop, pp. 55-61, 2003.
[5] A. K. Yadav, D. Singha and V. Kumar, "Forgery (Copy-Move) Detection In Digital Images using Block Method", International Journal of Collaborative Research in Engineering Sciences, (2014), April.
[6] Y. Ke, Q. Zhang, W. Min and S. Zhang, " Detecting Image Forgery Based on Noise Estimation" International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 1, (2014), pp. 325-336.
[7] D.G. Lowe, "Distinctive Image Features from Scale-Invariant Key points". International Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.
[8] A Survey of Digital Image Tampering Techniques Nishtha Parashar1 , Nirupama Tiwari2, Deepika Dubey3 1,2,3Computer Science & Engineering Dept., SRCEM, Banmore nishtha2909@gmail.com, girishniru@gmail.com2, deepika.sa1304@gmail.com
[9] W.-C. Hu et al., Effective composite image detection method based on feature inconsistency of image components, Digital Signal Process. (2015).
[10] https://en.wikipedia.org/wiki/Scale-invariant_feature_transform