International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 07 | Oct-2015 www.irjet.net p-ISSN: 2395-0072

A NOVEL IMAGE FORGERY DETECTION APPROACH BY USING SCALE INVARIANT FEATURE TRANSFORM

M.MEENAKSHI
PG Scholar
SNS College of Technology
Coimbatore, Tamilnadu ,India.
meenumahalingam@gmail.com

K.S.MOHAN
Assistant professor, IT Dept
SNS College of Technology
Coimbatore, Tamilnadu ,India.

ABSTRACT:

In recent years, more and more researchers have begun to focus on the problem of digital image tampering. One of the image tampering is copy-move forgery which is to paste one or several copied region(s) of an image into other part(s) of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image. In existing system, Adaptive Over segmentation and Feature Point Matching are used for detect the copy-move forgery. To improve the speed and accuracy of the system, the proposed system introduced a new method of image segmentation, named SLICAP, which combines the simple linear iterative clustering (SLIC) method with the affinity propagation (AP) clustering algorithm. Speeded Up Robust Features (SURF) used for extract features instead of Scale-Invariant Feature Transform (SIFT) from image block. Finally we propose the Forgery Region Extraction algorithm for detect the forgery region. Experimental results are presented to demonstrate the effectiveness of the proposed method.

KEY WORDS: *SLIC, AP, SURF, SIFT*

I.INTRODUCTION

Techniques for digital image tampering are becoming widespread for the availability of low cost technology in which the image could be easily manipulated. Copy-move forgery is one of the tampering techniques that are frequently used and has recently received significant attention.

At First, we employed the DWT method to the host image for obtain the coefficients and employed the SLICAP segmentation algorithm together for segment the host image which obtains the image blocks (IB).The block features are extracted by using Speeded Up Robust Features (SURF). Finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region. To detect the forgery regions more accurately, we propose the forgery region extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions. Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions.

II. Detecting Copy move Forgery using DCT

Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content, and detecting forgeries will only increase. Detection of malicious manipulation with digital images (digital forgeries) is the topic of this paper. In particular, we focus on detection of a special type of digital forgery – the copy-move attack in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image

feature. In this paper, we investigate the problem of detecting the copy-move forgery and describe an efficient and reliable detection method. The method may successfully detect the forged part even when the copied area is enhanced/retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG. The performance of the proposed method is demonstrated on several forged images.

III. Analysis of Copy-Move Image Forgery Detection

Highlight a section that Digital Image Forgery is a very important field in image processing. It is important because digital images are used in many social areas like in courts when they are used as evidence, medical imaging and journalism. The availability of powerful software tools such as Photoshop makes easy to manipulate the digital images. Over the past ten years, the field of digital forensics has proceeded in helping return some trust to digital images. Different techniques for maintaining the integrity of digital images have been developed. These techniques can be divided into two groups: intrusive and non-intrusive. In intrusive (active) techniques, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and authentication is done by verifying if the true signature matches the retrieved signature from the test image. Non-intrusive techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. There are three types of image forgery; Copy- Move, Image splicing and Image retouching. 1) In Copy- Move Forgery, one part of the image is copied and that part is pasted on other part of the same image to cover an important scene of the image. 2) In Image-Splicing, two images are combined to create one tampered image. 3) In Image Retouching the image is less modified. It just enhances some features of the image. Ethically it's also wrong.

IV. Detection of Region Duplication Forgery in Digital Images Using SURF

Nowadays, digital images are widely used in our society. From newspapers to the tabloid magazines, scientific journals, physicians in medical field, fashion industries, court rooms and other outlets heavily depend on digital images. Information integrity is fundamental in many fields. Historically we had confidence in the integrity of imagery; today's digital technology has begun to erode this trust. Even though tampering with photograph is not new, during the past few years, doctored images are appearing with growing frequency and sophistication. This is mainly due to the availability of low-cost hardware and photo editing software which makes it easy to manipulate and alter digital images without leaving any obvious trace. For an example recently, Egypt's state-run newspaper, *Al-Ahram,* published the altered photo of Egyptian President Mubarak walking with Israeli, US, Palestinian and Jordanian leaders during the latest Middle East peace talk.

V. Detecting Copy move Forgery using DCT

In today's world it is easy to manipulate the image by adding or removing some elements from the image which result in a high number of image forgeries. Using the manipulation tools that are available on internet it is easy to tamper the digital images without any trace. Therefore verification of originality of images has become a challenging task. An image can be manipulated with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. We need image forgery detection technique in many fields for protecting copyright and preventing forgery. In the proposed system detect region duplication forgery by applying Discrete Cosine Transform. We divide the image into overlapping blocks and then search for the duplicated blocks in the image. There is an approach that can detect doctored JPEG images and further locate the doctored parts, by examining the double quantization effect hidden among the DCT coefficients. Our method detects region duplication forgery by dividing the image into overlapping blocks and then we search for the matching region in the image. The result of the test is very encouraging since we got improvements in the detection rate and the detection time of the copy-move attack detection algorithm that we used. We are happy that the project is able to meet the outlined objectives proved that the use of DCT is better than using PCA for detecting copy-move attacks in highly textured images.

VI. An efficient and robust method for detecting copy-move forgery

Powerful digital media editing tools made it possible to produce good quality forgeries for almost anyone. One of the specific type of forgeries, which is the main interest of this system , is copy-move forgery, that can be done very easily by using the tools such as Cloning in Photoshop. This type forgery usually aims to cover an unwanted scene in the image, by copying another scene from the same image, generally a textured region, and pasting it onto the unwanted region. In this system, we propose a new approach for detecting copy-move forgery in digital images, which is considerably more robust to lossy compression, scaling and rotation type of manipulations. Also, to improve the computational complexity in detecting the duplicated image regions, we propose to use the notion of counting bloom filters as an alternative to lexicographic sorting, which is a common component of most of the proposed copy-move forgery detection schemes. Therefore, the utilized features should be insensitive to those operations as well. It should be noted that, the tampered can only afford to slightly rotate, scale or blur the duplicated image region. Aside from visual intactness considerations, since the type of traces introduced by these modifications depend on the strength of the modification, various other tamper detection techniques could be effectively used for their detection.

VII.FLOW DIAGRAM OF THE SYSTEM

First the input image is taken to identify the forgery region. Adaptive Over-Segmentation method can determine the initial size of the super pixels adaptively based on the texture. First, we employed the DWT to the host image to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, we calculated the percentage of the low-frequency distribution P_{LF} according with initial size S . Finally, we employed the SLIC segmentation algorithm together with the calculated initial size S to segment the host image to obtain the image blocks (IB). fig3 shows the Adaptive Over-Segmention.

Block features are extracted from image blocks. Feature points are extracted from each block as block features and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression.

SIFT is used as the feature point extraction method to extract the feature points from each image block. Each block feature contains irregular block region information and the extracted SIFT feature points.

Block feature is composed of a set of feature points. The number of blocks are matched and calculated adaptively with the result, the matched block pairs are located; and finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region.

Labeled feature points are extracted which are the locations of the forgery regions. To obtain suspected region we have to replace the LFP with small super pixels.

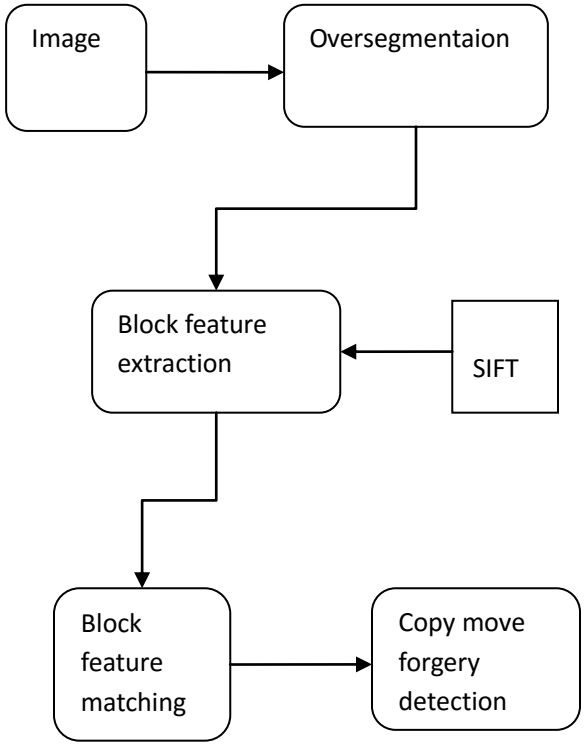

fig1 shows the flow diagram of the system

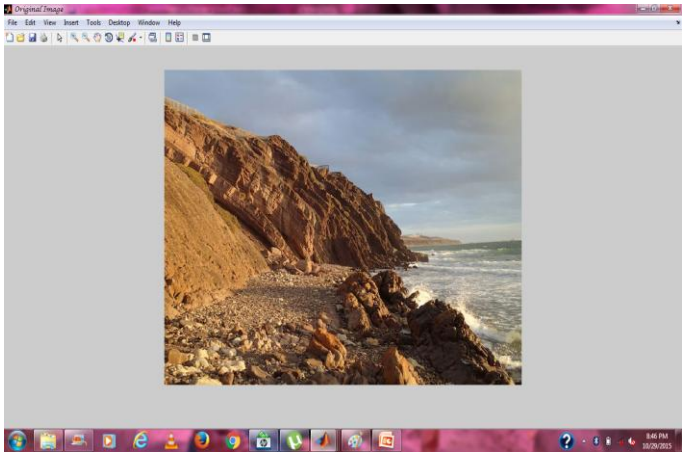

fig 2 shows the original image

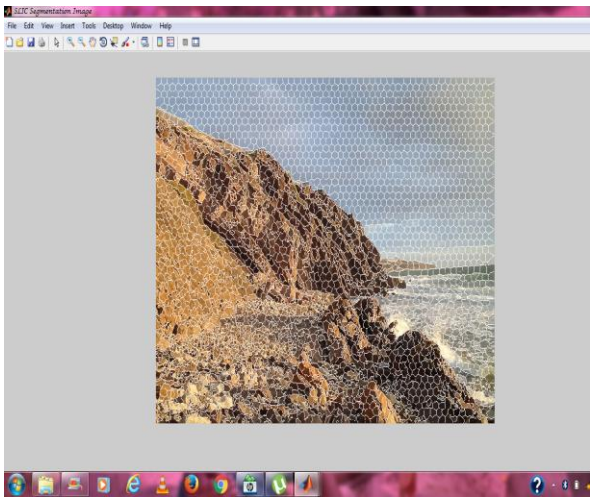

fig3 shows the adaptive over segmentation

VII. CONCLUSION

In this paper, a new method for illumination and feature extraction has been proposed. Speed and accuracy of the system is improved by using Simple Linear Iterative Clustering and Affinity Propagation and Scale Invariant Feature Transform. Block by Block Feature Extraction paired face feature to detect the spliced image from the original image.

REFERENCES

[1]B.L.Shivkumar and Lt.Dr.S.Santhosh Baboo,"Detection of Region Duplication Forgery inDigital Images Using SURF".
[2] M. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in *Proc. Int.Workshop on Inform. Hiding*, 2007, pp. 311–325.
[3] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Dec. 2010, pp. 1–6.
[4] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "3D lighting-based image forgery detection using shape-from-shading," in *Proc. Eur. Signal Processing Conf. (EUSIPCO)*, Aug. 2012, pp. 1777–1781