ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Forgery Detection Technique Based on Block and Feature Based Method

Tushant A. Kohale[1], Dr. S.D. Chede[2], Prof. P.R.Lakhe[3]

Department of Electronics (Comm. Engg.), S. D. College of Engg. Wardha, India[1]

Depatment of Electronics & Telecom. Engg., Om College of Engg. Wardha, India [2]

Department of Electronics (Comm. Engg.), S. D. College of Engg. Wardha, India[3]

Abstract: Digital images are the most important source of information. The availability of powerful digital image processing software's, makes it relatively easy to create as well as manipulate and make digital forgery from one or multiple images. In today's world it is easy to developed the image forgery by adding or removing some elements from the image which result in a of image tampering. A copy-move forgery is created by copying and pasting content within the same image, and post-operating it. The detection of copy-move forgeries has become one of the most actively researched topics in image forensics department. The key objectives of the proposed method is to study the effect of different types of tampering on the digital image, detect image forgery by copy-move under many types of attacks by combining block-based and feature based method and accurately locating the duplicated region.

Keywords: image, image forgery, copy-move image forgery detection, block and feature based methods.

I. INTRODUCTION

Digital images are the most important way for transfer information, so the integrety of images are very essential. Due to advances and availabilities of powerful image processing software's, it is easy to manipulate and create digital image forgery. Adding and deleting content from an image is most easiest and popular way of creating image forgery. Copy move is one of the type of digital image forgery. In order to identify the integrity of the images we need to detect any modification on the image. Digital Image Forensics is the field that deals with the authenticity of the images. Digital image forensics checks the integrity of the images by detecting various forgeries.

II. MOTIVATION

Copy-move is a simple and effective technique to make image forgeries in the digital image. In this forgery type a part of the image is copied and pasted to another part of the same image. Copy-move simply requires the pasting of image blocks in same image and hiding important information from the image. Thus, this changes the originality of the image. Digital image forgery detection techniques are classified into active and passive approaches. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image. In passive approach, do not require any prior information about the image and depends on traces left on the image by different processing steps during image manipulation.

A number of techniques proposed to detect copy-move forgery which can be classified into two main categories such as block-based and key point-based methods. Good forgery detection method should be robust to manipulations, such as scaling, rotations, JPEG compression and Gaussian Noise addition made on the copied content. These attacks are not detected by the single method. The novel approach is proposed to detect image forgery by copy-move under above attacks by integrating block-based and feature-based method.to it.

III. RELATED WORK

Fridrich, D. Soukal, and J. Lukas investigated the problem of detecting the copy-move forgery and mentioned an efficient and reliable detection method. The method detect the forged part even when the copied area is enhanced or retouched. Discrete Cosine Transform (DCT) which isblock based used for the detection. For each block, the DCT transform is calculated and quantized. Then coefficients are matched with each other. However this method fails for any type of geometrical transformations of the query block e.g. rotation; scaling [1]. A.C. Popescu and H. Farid proposed Principal Component Analysis (PCA). This method is robust to minor variations in the image due to additive noise or lossy compression. Duplicated regions are then detected by lexicographically sorting all of the image blocks. This technique is effective on plausible forgeries, and has quantified its sensitivity to JPEG lossy compression and additive noise [2]. Xunyu Pan & Siwei Lyu described a method to detect duplicated and distorted regions based on the robust matching of image key points. Though having achieved performance in detecting sophisticated forgeries with duplicated regions, this method relies on the detection of reliable SIFT's key points. For some images this may be a limitation. Because smaller regions have fewer key points, they are hard to detect with SIFT method. Second, this method fails for images that have intrinsically identical areas that cannot be differentiated from intentionally inserted duplicated regions [3]. S.Murali, Basavaraj S. Anami, Govindraj B. Chittapur proposed methodology to identify photo images and succeeded to identify forged region by giving only forged photo image as input image. The proposed method effectively detecting photo image forgery which is supported to both copy-move image forgeries. Methodology based on JPEG compression

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

analysis and direction filter using jpeg image analysis. This method captures the forged area after using various threshold values for testing. The larger threshold value effectively filters out the false positives caused by edges since tampering with an area on the image usually causes greater variability in the JPEG blocks. [4]. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra proposed the method of detection using scale invariant feature transform (SIFT) key point. In this paper, the problem of detecting if an image has been forged is investigated in particular, attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create duplication. Generally, to adapt the image patch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on Scale Invariant Features Transform (SIFT) is proposed. Such a method allows both to understand if a copy-move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. It detects the key point and match them using nearest neighbour search. This method is robust to rotation and scaling but cannot detect forgery by smooth surfaces [5]. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou analysed the different algorithms and to evaluate their performance of different widely-used features for copy-move forgery detection. As a result it was shown that different keypoint-based methods like SIFT and SURF, and block-based methods like DCT, PCA, KPCA, DWT, perform.

IV. PROPOSED METHODOLOGY

- Apply SIFT on image for finding and locating key-points
- Apply Sift on image with different attack of tampering
- Creating image forgery for tampering
- Detect tampering location using block-DCT and feature SIFT

A. Feature extraction using Image key point

SIFT is the first stage of proposed method, which is used to finding the image key points.This approach has been named the Scale Invariant Feature Transform (SIFT), as it transforms image data into scale-invariant coordinates relative to local features. This mainly concerned with finding key points, by converting RGB image into grayscale image. Here, we present a new region duplication detection method based on the image SIFT features, we first detect SIFT key points in an image and compute the SIFT features for such key points. At each key point, a 128 dimensional feature vector is generated from the histograms of local gradients in its neighborhood.

Output of SIFT:

Time for Gaussian scale space construction: 6.665 s

Time for Differential scale space construction: 0.018 s

Time for finding key points: 0.363 s

Toatl numer of key points extracted are : 1452

Time for calculating descriptor: 1.661 s

B. Locating Duplicated Region

This is the stage in which we obtain the duplicated region. By integrating block based and feature based method. For locating more duplicated region in forgery images, we run our detection method iteratively with each iteration selecting one pair of potential duplicated regions. As the last step, all recovered duplicated regions are combined together and mapped back to the original image coordinates. Figure:1 shows the the duplicated region which is translated to the target location with no distortion and also locating its region. And figure:2 shows the graphical representation of it.

Fig-1: Image forgery example.

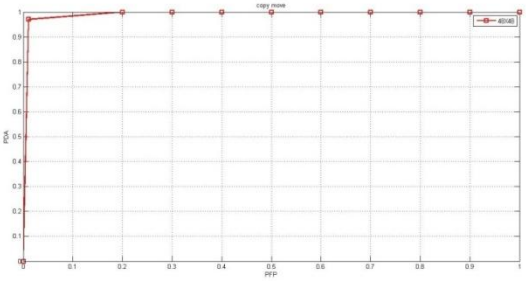

Fig-2: Graph representation of image forgery.

V. CONCLUSION

In this paper a method for digital image forgery detection is based on block based and feature based method. The Proposed methodology is a combination of block-based and feature-based method and able to detects combination of number of postoperation by single method. By integrarting this method if one method fails to detect forgery then other method detects it and vice-versa and the detection rate and efficiency will increase. This method is mostly used to detection of manipulation with image called image forgery in case of copy move.

REFERENCES

[1] S. J. Fridrich, D. Soukal, and J. Lukas,"Detection of copy-move forgery in digital images," *Proceedings of Digital Forensic Research Workshop, Aug. 2003*.

[2] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Technical Report TR2004-515*, Dartmouth College, 2004.

[3] Xunyu Pan & Siwei Lyu, student member , IEEE "Region duplication detection using image feature matching" *IEEE Transaction on information forensics and security*,vol.5, No.4 December 2010

[4] S.Murali, Basavaraj S. Anami, Govindraj B. Chittapur "Detection of Digital Photo Image Forgery"*2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)* M. Shell. (2002)

[5] Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[6] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1841-1854, 2012.