Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection of Postoperated Copy Move Image Forgery by Integrating Block Based and Feature Based Method

Tushant A. Kohale*, Prof. P. R. Lakhe
Department of Electronics Engineering (Comm.)
RTM Nagpur University, India

Dr. S. D. Chede
Department of Electronics & Telecom. Engineering
RTM Nagpur University, India

Abstract*— Digital images are the most important source of information transfer. The availability of powerful digital image processing software's, makes it relatively easy to create digital forgeries from one or multiple images. 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. A copy-move forgery is created by copying and pasting content within the same image, and potentially post-operating it. The detection of copy-move forgeries has become one of the most actively researched topics in blind image forensics. The key objectives of the proposed approach 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*— digital image, image forgery, image forensic, copy-move forgery detection, block based and feature based methods.

I. INTRODUCTION

Digital images are the most prevalent way to convey information, so the authenticity of images is very essential. Due to rapid advances and availabilities of powerful image processing software's, it is easy to manipulate and modify digital images. Adding and deleting content from an image is most easiest and popular way of creating 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.

Figure 1: Example of copy move forgery. Left: The original image. Right: The tampered image.

Copy-move is a simple and effective technique to create image forgeries in the digital image. In this technique 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 and put at stake the authenticity of that 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.

© 2014, IJARCSSE All Rights Reserved

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.

II. RELATED WORK

Fridrich, D. Soukal, and J. Lukas investigated the problem of detecting the copy-move forgery and described an efficient and reliable detection method. The method 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 .Discrete Cosine Transform (DCT) used for the detection. It begins from upper left corner to the lower right corner while sliding a B×B block. 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) on small fixed-size image blocks to yield a reduced dimension representation. This representation 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 and features. Though having achieved promising 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. The proposed method effectively detecting photo image forgery which is supported to both copy-move and copy-create type of image forgeries. Methodology based on JPEG compression 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 or to cancel something that was awkward. 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 well and they can be combined as to get better result [6].

III. PROPOSED METHODOLOGY

In this paper, proposed method detects the copy move region in the following modules:

A. Detection using block based method

The block based method, especially DCT (Discrete Cosine Transform) are invariant to JPEG compression and Gaussian noise addition. Divide the image into small overlapping blocks and extract a few descriptive features from each block. A decision is made as to whether the image contains a forgery based on matching blocks.

B. Feature extraction using Image key point

In this module, first of all we have to find Image Key point which carries distinct information of an Image. Scale Invariant Feature Transform (SIFT) is an algorithm for obtaining effective Key point. SIFT are used for illumination changes in an image to find the copy-move region. Feature vector is generated at each Key point from the histogram of local gradients in its neighbourhood. Using Best-bin-first algorithm, SIFT Key point are matched on the basis of their feature vectors.

C. Estimation of Affine Transform

This module deals with the possible geometric distortions of the copy-move region. We can use putative matching of SIFT Key point to estimate the affine transform parameter, but the obtained results are inaccurate due to large number of mismatched Key point. Weed out of unreliable key points and for accurate transform parameters; we are using robust estimation method known as Random Sample Consensus (RANSAC) algorithm. It can estimate the model parameters with a high degree of accuracy even when a significant number of mismatched pairs are present.

© 2014, IJARCSSE All Rights Reserved

D. Locating Duplicated Region

This is the final module in which we obtain the duplicated region by region correlation. After that Gaussian filter is used to reduce the noise in correlation maps. 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

IV. CONCLUSIONS

In this paper a method for forgery detection in digital image based on block based and feature based method is used. The Proposed methodology is a combination of block-based and feature-based technique and able to detects combination of number of post-processed operations by single method. Using this method, if one technique fails to detect forgery then other technique 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.

ACKNOWLEDGMENT

I would like to thank my guide Prof. P. R. Lakhe, and Dr. S. D. Chede for their guidance and support and Department of Electronics Engineering (Comm.), S. D. College of Engineering, Wardha.

REFERENCES

[1] 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)*

[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

© 2014, IJARCSSE All Rights Reserved