An Improved Forgery Image Detection Method by Global Region-based Segmentation

Geofrey Katema
Dept. of Electronics Engineering
Tianjin University of Technology and Education
Tianjin, P,R China

Prof. Lili
Dept. of Electronics Engineering
Tianjin University of Technology and Education
Tianjin, P.R China

***Abstract*-Chinese proverb says image say more than thousand words; this saying proves that image is of very big importance of what it portrays to the society. Digital images are everywhere and are useful for information whether in court for justice issues or in sport or anywhere. With advancement of technology the image can now be easily tampered which bring its authenticity into question. With the training image and test image we propose the passive (blind) detection method for copy-move forgery by the improved preprocessing Global region-based segmentation with the SIFT feature keypoint matching to detect and localize the forgery. The output of the proposed method with different datasets show fantastic results with improved efficiency compared with other earlier methods. This work is going to classify the original and tampered image hence bring the truth to the light, and also to add contribution to the forensic research area.**

Key words: Digital Image, Copy- move forgery, region-based segmentation, feature matching.

I .INTRODUCTION

For quite a time now Images have been used for different purposes in the society and due to its trustworthiness it has also been used as evidence in court rooms where the reliable evidence is of primary importance. Not only that but also in the medical field as well doctors have used images for diagnosis of different diseases and in areas like military, forensic, media, sports as well as in science they both use the images for their development and detection of any change in the monitored field. The advancement in the technology which sees the low-cost advanced digital camera and the image processing software changes the market and the Image has become easily altered which is difficult to see by our necked eyes and thus compromises its trustworthiness. Whole process of image manipulation is thus called Image forgery this can be copy-move [1].

So the image forgery process challenges the reliability and authenticity of the image presented to the court as evidence, in medical diagnosis as well as in the newspapers or media due to the difficulty of differentiating the original and modified image which in turn lead the people believing in a wrong message as to the saying that the seeing is believing but here will be believing the wrong information to be true and make bad influence to the society.

Since the attack of image forgeries has come to exposition, so it a calls for a reliable forgery detection system for digital images to prove the image authenticity. Digital image forgery detection techniques are classified into active and passive approaches [2]. This paper deals with the passive approach whereby it makes improvement to the output efficiency of the image forgery detection (copy-move). By improving especially the preprocessing part of the image processing followed by Scale Invariant Feature Transform (SIFT) [3] the efficiency is remarkable. Figure below shows the example of copy-move forgery.

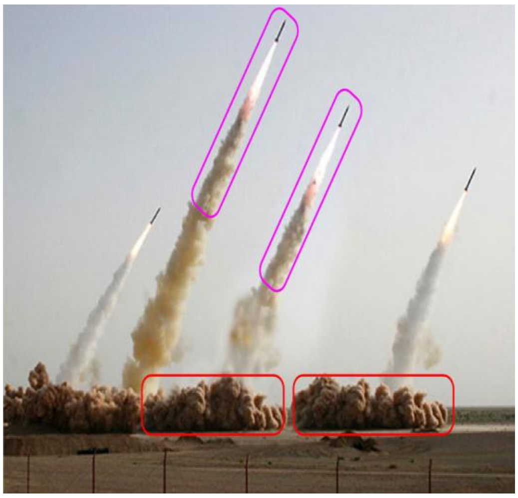

Fig.1. an example of image tampering that appeared in press in July, 2008. The feigned image (on the right) shows four Iranian missiles but only three of them are real; two different sections (encircled in red and purple, respectively) replicate other images sections by applying a copy-move manipulation.

II. RELATED WORK

In [2] discussed different detection method on different image forgeries which has already been done and one of them is the copy-move forgery, explained and show how they perform with their percentage indicated. But most interestingly is about Xunyu and Siwei [4] presented a technique that uses region duplication by means of estimating the transform between matched SIFT key points that is invariant to distortions that occurs due to image feature matching and showed high percentage of accuracy. There many different works done to date, all is to find the most robust algorithm which can work on both ways of forgeries.

SIFT features are detected at different scales using a scale-space representation implemented as an image pyramid [13]. The pyramid levels are obtained by Gaussian smoothing and sub-sampling of the image resolution while interest points are selected as local extrema (min/max) in the scale-space. These key points, referred to as x_i in the following, are extracted by applying a computable approximation of the Laplacian of Gaussian called Difference of Gaussians (DoG). Specifically, a DoG image D is given by: $D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) = L(x, y, k\sigma) - L(x, y, \sigma)$, where $L(x, y, k\sigma)$ is the convolution of the original image $I(x, y)$ with the Gaussian blur $G(x, y, k\sigma)$ at scale $k\sigma$. In order to guarantee invariance to rotations, the algorithm assigns to each keypoint a canonical orientation o. To determine this orientation, a gradient orientation histogram is computed in the neighborhood of the keypoint. Specifically, for an image sample $L(x, y, \sigma)$ at scale σ (the scale in which that keypoint was detected), the gradient magnitude $m(x, y)$ and orientation $\theta(x, y)$ are precomputed using pixel differences:

$$m(x, y)=(((L(x+1, y)-L(x-1, y))^2 + ((L(x,y+1)-L(x, y-1))^2)^{1/2}, \quad (i)$$

$$\theta(x, y)= \tan^{-1}((L(x, y+1)-L(x, y-1))/(L(x+1, y)-L(x-1, y)), \quad (ii)$$

Summarizing the above, given an image I, this procedure ends with a list of N key points each of which is completely described by the following information: xi = {x, y, σ, o, f}, where (x, y) are the coordinates in the image-pyramid used to compute the descriptor), o is the canonical orientation (used to achieve rotation invariance) and f is the final SIFT descriptor.

III. PROPOSED METHOD

In this algorithm we first need to have training image set and the test image whereby we first load the training image and after that we convert to gray scale image followed by Global region-based segmentation followed by some post processing then we sport out the object and after that by using SIFT feature detection we do feature extraction based on extracted feature the classifier is set and most the classifier is to classify an image whether is original or forged and as well localize such forgery. The most important here is the preprocessing and we also see segmentation which is done using the Global Region – based segmentation, the aim of preprocessing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing or image analysis.

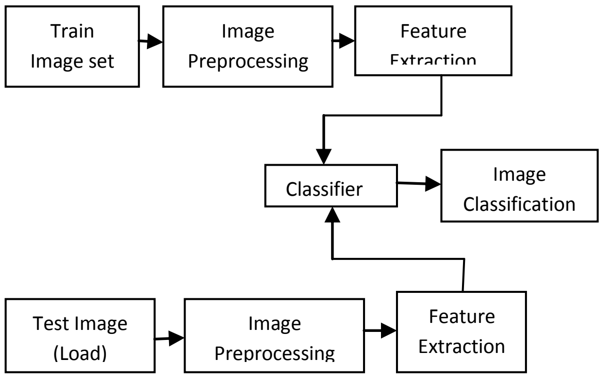

Fig.1. General Structure of image forgery detection

A. Global region-based segmentation

Segmentation partitions an image into distinct regions containing each pixel with similar attributes. To be meaningful and useful for image analysis and interpretation, the regions should strongly relate to depicted objects or features of interest. Meaningful segmentation is the first step from low-level image processing transforming a grayscale or colour image into one or more other images to high-level image description in terms of features, objects, and scenes. The success of image analysis depends on reliability of segmentation, but an accurate partitioning of an image is generally a very challenging problem [5]. Region-based approaches try to find partitions of the image pixels into sets corresponding to coherent image properties such as brightness, color and texture. This gives rise to proto-surfaces. This is important for a number of reasons (1) surfaces are the natural units of perception [6]. Region-based techniques usually involve defining a global objective function (for example, Markov random fields [7] or other variational formulations [8]). The advantage of having a global objective function is that hard decision are made only when information from the whole image is taken into account at the same time [9]

B. *Feature extraction*

Most of the algorithms proposed in the literature for detecting and describing local visual features usually requires two steps. The first is the detection step, in which interest points are localized, while in the second step robust local descriptors are built so as to be invariant with respect to orientation, scale and affine transformations. From a comprehensive analysis of several local descriptors [10] and local affine region detectors surveyed in [11] confirm that SIFT features [12] are a good solution because of their robust performance and relatively low computational costs. Since SIFT features are robust to scaling, rotation and affine transformations that are well-suited for the detection of copy-move forgeries as has been recently demonstrated in [14, 13]. We detect keypoints that are stable local extrema in the scale space and, for each of them, a feature vector is computed from a local pixel area around the detected point. Given a test image I, let S: = $fs_1; : : : ;s_ng$ be the list of n interest points taken from this image, where s_i = $fx_1; f_ig$ is a vector containing the keypoint coordinates x_i = (x, y) and f_i is the feature descriptor of the local patch around the keypoint (i.e an histogram of gradient orientations of 128 elements). In presence of a copy-move manipulation the extracted SIFT keypoints from the copied and the original regions have similar descriptor vectors. Therefore, matching among SIFT features is adopted to detect if an image has been tampered with and, subsequently, localize such forgery

IV. EXPERIMENTAL RESULTS

In experiment the Matlab codes were used for the whole procedure and processes. The experiments were conducted mainly in two parts the preprocessing i.e the change of image in gray scale image, segmentation and then the object detection after that then comes the other part which is SIFT feature matching, classifier selection and lastly detection.

(a) Preprocessing outputs

In this stage we take the original image which we treat it as the train image and it undergoes the trend of the preprocessing before we extract its features by SIFT algorithm for maximum feature extraction from it.

Fig.2. Loaded image

Fig.3. Gray scale image

Fig.4. Segmented image

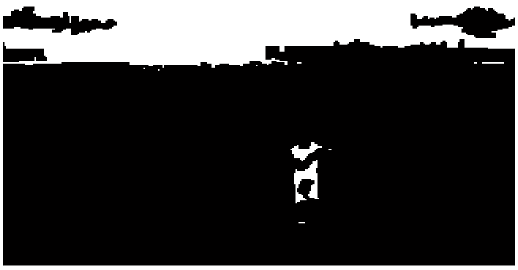

Fig.5. Postprocessed segmented image

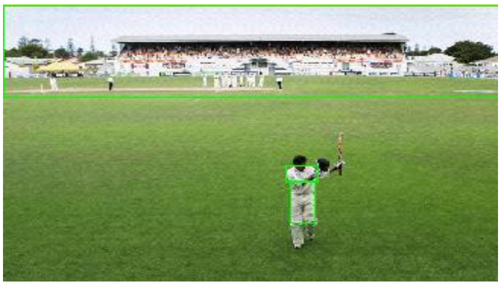

Fig.6. Object detection

(b) SIFT feature detection and the Final output result with the localized forgery part clearly shown.

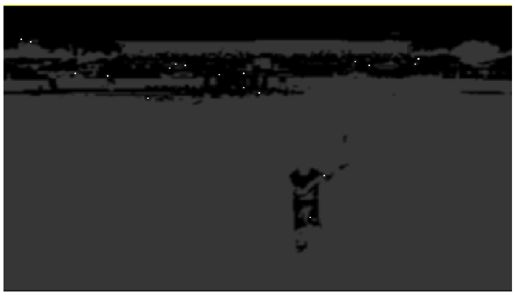

Fig.7. Image with keypoint mapped onto it

Below is the Forged image which will be loaded as the test image to the algorithm (Matlab code) to be checked for its authenticity. We expect after this procedure to be able to even see the area where mostly the forgery has happened or the information has been concealed

Fig.8. Test image

Fig.9. Test image with keypoint mapped onto it

Fig.10. Detected forged image with the localized forgery

So from the train image to the test image and all the processing stages, the results here shown explains that we can be assured that with this proposed method of forgery detection especially copy-move detection is achieved with maximum efficiency and from just this sample of original and forged image the percentage of forgery or tempering was found just to be 3.000%

V. CONCLUSION

Copy-move forgery is very common in our daily life this paper has introduced the work of detection by use of passive (blind) method where by the improved segmentation has shown great improvement of feature detection by using SIFT feature algorithm and hence improved the efficiency of forgery detection and as well to localize the forgery. This work being among other work done in the field of forensic where it helps the researches and contributes to the search of the robust algorithm and method to obtain the perfect image forgery detection of any kind of forgery with maximum possible efficiency.

VI. REFERENCES

(1) Ms. P.G Gomase, Ms. N. R. Wankhade "ADVANCED DIGITAL IMAGE FORGERY DETECTION: A REVIEW" IOSR Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-8727 PP 80-83
(2) Saba Mushtaq and Ajaz Hussain Mir"Digital Image Forgeries and Passive Image Authentication Techniques: A Survey" International Journal of Advanced Science and Technology Vol.73 (2014), pp, 15-32
(3) D.G. Lowe, Distinctive image features from scale-invariant key points, Int.'1 Journal of Computer Vision 60 (2) (2004) 91-110.
(4) P. Xunyu and L. Siwei, "Region duplication detection using image feature matching", IEEE Trans Inf Forensics Security, vol. 5, no. 4, (2011), pp. 857-67
(5) www.cs.auckland.ac.nz/courses/compsci/773slc/lectures/image
(6) K.Nakayama and S. Shimojo. Experiencing and perceiving visual surfaces. Science, 257, Sept 1992.
(7) S.Geman and D.Geman. Stochastic relaxation, gibbs distribution, and the Bayesian restoration of images. IEEE Trans. PAMI., 6, Nov. 1984
(8) D. Mumford and J. Shah. Optimal approximations by piecewise smooth functions, and associated variational problems. Comm. Pure Math., 1989
(9) Thomas Leung and Jitendra Malik" Contour continuity in region based image segmentation" H. Burkhardt. B. Neumann (Eds.): Computer Vision -ECCV '98, Vol 1, LNCS 1406, pp. 544-559
(10) K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 10, pp. 1615–1630, 2005.
(11) K. Mikolajczyk, T. Tuytelaars, C. Schmid, A. Zisserman, J. Matas, F. Schaffalitzky, T. Kadir, and L. Van Gool, "A comparison of affine region detectors," International Journal of Computer Vision, vol. 65, no. 1/2, pp. 43–72, 2005.
(12) D. G. Lowe, "Distinctive image features from scale-invariant key points," Int.'l Journal of Computer Vision, vol. 60, no. 2, pp. 91–110, 2004.
(13) Irene Amerini, Lamberto Ballan, Student Member, IEEE, Roberto Caldelli, Member, IEEE, Alberto Del Bimbo, Member, IEEE, and Giuseppe Serra "A SIFT-based forensic method for copy-move attack detection and transformation recovery" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
(14) Xunyu Pan *Student Member, IEEE*, and Siwei Lyu, *Member, IEEE* "Region Duplication Detection Using Image Feature Matching" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER 2010