IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 4, April 2018

A New Method for Image Forgery Detection

Sreemol R[1]

M. Tech in Computer Science and Engineering, CSE, Rajiv Gandhi Institute of Technology, Kottayam, India[1]

Abstract: Digital Images are source of information. In Image Forensics, the detection of copy- move forgery detection has received much more attention. In the case of Copy- Move Forgery, the same part of the image is copied and pasted into some other parts of the same image itself. So, it is very difficult to identify such forged regions since the color, contract and other features are almost similar to the original image. In this work, the copy –move forgery detection is identified using Adaptive Oversegmentation and feature point matching. It combines the advantages of both Block based and Keypoint based forgery detection techniques. The image is divided into different blocks using Adaptive Oversegmentation. Then, the feature points are extracted from each block as block features, and the block features are matched with one another. If the match value exceeds the predefined threshold value, the suspected forgery regions will be indicated. Merged Regions are extracted using Forgery Region Extraction Algorithm. To generate the detected forgery regions the morphological operation is applied to the merged regions.

Keywords: Feature point, Forgery, Image, Keypoint, Oversegmentation

I. INTRODUCTION

Due to the development of technology, image forgery in digital images is very easy to perform. Copy Move Forgery is one of the important image tampering. The part of the image is copied and pasted into the same image itself. So, it is very difficult to identify such image tampering. Because, the features of the parts which are copied will be almost similar to that of the original image Copy Move Forgery detection techniques are of two types: Block Based Methods and Feature Keypoint Methods. Block based methods divide the images into overlapping regular blocks. In key point based methods, where image keypoints are extracted and matched over the entire image to resist some image transformations while identifying duplicated regions. In this work, a new method is proposed which divides the entire image into non-overlapping-irregular blocks. All existing block-based forgery detection systems segment the image into regular overlapped blocks. This will limit the forgery detection results because it cannot detect significant geometrical transformations of the forgery regions. Also computational cost increases when the size of the image increases. Size and shape of each segment will affect the accuracy of forgery detection results. Although these advantages can overcome by keypoint based algorithms, their recall rate is very low. Proposed scheme will integrate both these techniques so that it can take the advantages of each method.

II. THE PROPOSED FORGERY DETECTION SCHEME

Image forgery detection is driven by the need of authenticity and to maintain integrity of the images. And in most of the cases copy- move image forgery is used to tamper the digital image, 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.

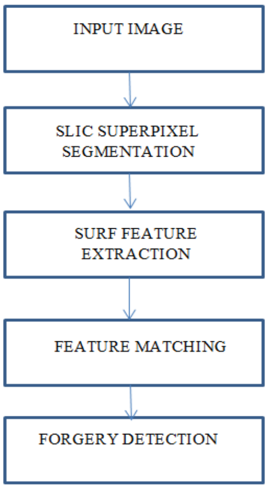

Fig. 1 Framework of the proposed Forgery Detection Scheme

DOI 10.17148/IJARCCE.2018.7469

Proposed system detects copy-move forgery in digital images using adaptive over segmentation and feature point matching. It integrates both block-based and key point-based forgery detection methods. Adaptive over segmentation algorithm segments the image into different blocks. Then, the feature points are extracted from each block as block features, and the block features are matched with one another, if the match exceeded the preset threshold it will indicate the suspected forgery regions. Using forgery region extraction algorithm, merged regions are generated. Finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. Fig.1 shows the overall architecture of the proposed system.

A. Segmentation

To segment the host image into non- overlapping regions of irregular shape and because the superpixels are perceptually meaningful atomic regions that can be obtained by over-segmentation, Simple Linear Iterative Clustering (SLIC) algorithm is employed to segment the host image into meaningful irregular superpixels, as individual blocks. The SLIC algorithm adapts a k-means clustering approach to efficiently generate the superpixels, and it adheres to the boundaries very well. Using the SLIC segmentation method, the non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocking; also, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the superpixels in SLIC is difficult to decide. Different initial sizes of the superpixels can produce different forgery detection results; consequently, different host images should be blocked into superpixels of different initial sizes, which is highly related to the forgery detection results. When the initial size of the superpixels is too small, the result will be a large computational expense; otherwise, when it is too large, the result will be that the forgery detection results are not sufficiently accurate. Therefore, a balance between the computational expense and the detection accuracy must be obtained when employing the SLIC segmentation method for image blocking. Here determine the initial size of the superpixels adaptively based on the texture of the host image. When the texture of the host image is smooth, the initial size of the superpixels can be set to be relatively large, which can ensure the superpixels will contain sufficient feature points to be used for forgery detection. A four-level Discrete Wavelet Transform (DWT) is employed, using the Haar wavelet, on the host image; then, the low-frequency energy E_{LF} and high-frequency energy E_{HF} can be calculated using Eqn.(1) and (2) respectively. With the low-frequency energy E_{LF} and high frequency energy E_{HF} , the percentage of the low-frequency distribution P_{LF} is calculated using Eqn.(3), according to which the initial size S of the superpixels can be defined as in Eqn.(4).

$$E_{LF}=\sum |CA_4| \qquad (1)$$

$$E_{HF}=\sum_i \sum |CD_i| + \sum |CH_i| + \sum |CV_i| \qquad (2)$$

where i = 1,2..4 and CA_4 indicates the approximation coefficients at the 4th level of DWT; and CD_i , CH_i and CV_i indicate the detailed coefficients at the ith level of DWT, i = 1, 2, ., 4.

$$P_{LF}={}^{E_{LF}}/_{E_{LF}} + E_{HF}\ .\ 100\% \qquad (3)$$

$$S=\begin{cases} \sqrt{.02 * M * N} & P_{LF}>50\% \\ \sqrt{.01 * M * N} & P_{LF}<50\% \end{cases} \qquad (4)$$

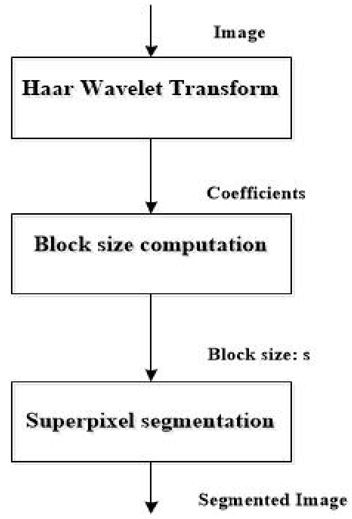

Fig. 2 Segmentation Block Diagram

S means the initial size of the super pixels; M*N indicates the size of the host image; and P_{LF} means the percentage of the low-frequency distribution. In summary, the flow chart of the adaptive over-segmentation method is shown in Fig.2. First, DWT is employed to the host image to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, the Percentage of the Low-Frequency distribution PLF is calculated using Eqn. (3), according to which the initial size S is determined, using Eqn. (4). Finally, SLIC segmentation algorithm is employed together with the calculated initial size S to segment the host image to obtain the Image Blocks (IB).

B. Feature Extraction

In this section, block features are extracted from the Image Blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features; however, those features mainly reflect the content of the image blocks, leaving out the location information. In addition, the features are not resistant to various image transformations. Therefore, feature points from each image block are extracted as block features, and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression. In recent years, the feature points extraction methods SIFT and SURF have been widely used in the field of computer vision. The feature points extracted by SIFT and SURF were proven to be robust against common image processing operations such as rotation, scale, blurring, and compression; consequently, SIFT and SURF were often used as feature point extraction methods in the existing keypoint-based copy-move forgery detection methods. SURF is chosen as the feature point extraction method to extract the feature points from each image block because of its low computational cost. Each block is characterized by the SURF feature points that were extracted in the corresponding block. Therefore, each block feature contains irregular block region information and the extracted SURF feature points.

C. Feature Matching

After obtaining the Block Features (BF), we must locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. Here, because the block feature is composed of a set of feature points, different method is used to locate the matched blocks. First, the number of matched feature points is calculated, and the correlation coefficient map is generated; then, the corresponding block matching threshold is 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.

D. Forgery Region Extraction

In feature-matching the Labeled Feature Points (LFP) should be obtained, which are only the locations of the forgery regions. To locate the forgery regions, the LFP are replacing with small superpixels. These are called to be suspected regions (SR), which are combinations of labeled small superpixels. To improve the precision and recall results, the local color feature of the superpixels that are neighbors to the Suspected Regions (SR) is to be measured; if their color feature is similar to that of the suspected regions, then merge the neighbor superpixels into the corresponding suspected regions, which generates the Merged Regions (MR). Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions.

III. EXPERIMENTS AND RESULTS

A series of experiments are conducted to evaluate the effectiveness and robustness of the proposed image forgery detection scheme. In the following experiments, the image dataset in [16] is used to test the proposed method. This dataset is formed based on 48 high-resolution uncompressed PNG true color images, and the average size of the images is 1500 x 1500. Fig. 3 shows the image produced using copy move forgery and Fig. 4 shows the copy-move forgery detection results of the proposed scheme. The two characteristics precision and recall are used to evaluate the performance of the proposed forgery detection scheme

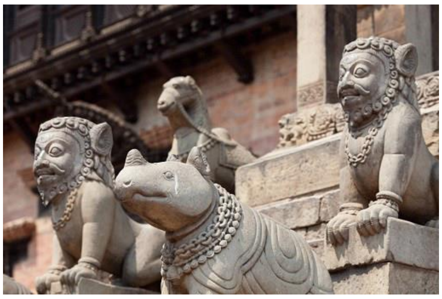

Fig. 3 Forgery Input Image

DOI 10.17148/IJARCCE.2018.7469

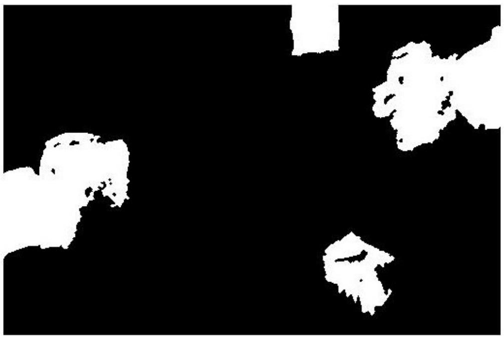

Fig. 4 Forged Areas

Precision is the probability that the detected regions are relevant, and it is defined as the ratio of the number of correctly detected forged pixels to the number of totally detected forged pixels. Recall is the probability that the relevant regions are detected, and it is defined as the ratio of the number of correctly detected forged pixels to the number of forged pixels in the ground truth forged image.

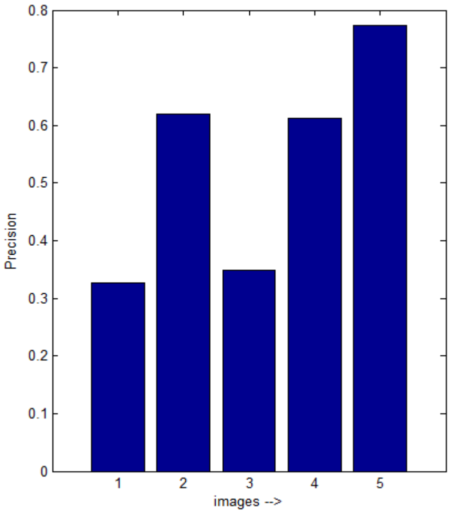

Fig. 5 Precision Graph

In addition to the precision and recall, F1 score is also used as a reference parameter to measure the forgery detection result; the F1 score combines both the precision and recall into a single value, and it can be calculated using:

$$\mathrm{F1} = 2 * \frac{\mathrm{Precision} - \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}} \tag{5}$$

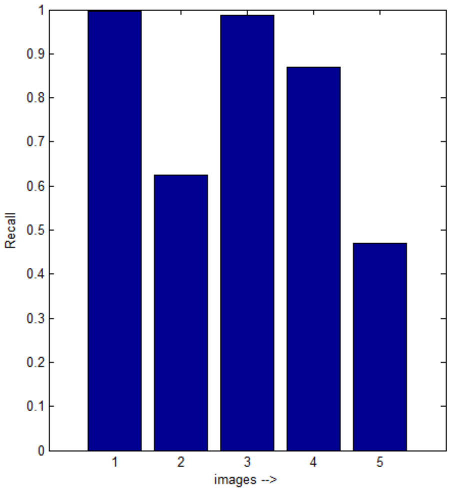

Fig. 5 Recall Graph

To reduce the effect of the randomness of the samples, the average precision and recall are computed. Evaluation of the method is done at the pixel level. At the pixel level, the precision and recall are calculated by counting the number of pixels in the corresponding region. In general, a higher precision and a higher recall indicate superior performance. So a better scheme will give a higher F1 score value.

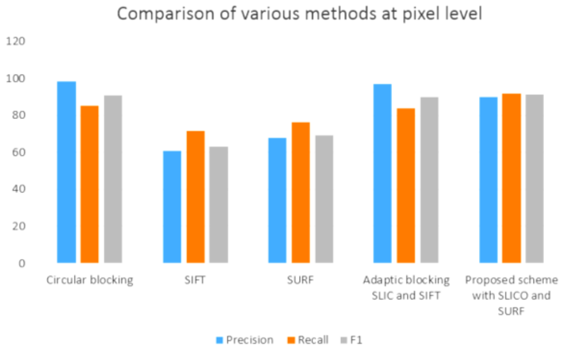

Fig. 6 Analysis of different methods

Fig.6 shows the average Precision, Recall and F1 score values of different copy-move forgery detection scheme including the proposed scheme. And among all, the proposed method has the highest value for F1 score. Comparison in account of time also the proposed method is better. Because for feature extraction there are mainly two algorithms: SIFT and SURF. SURF is faster than SIFT. In this method, SURF is used for feature extraction. Only less computational time is needed. So it will give detection results faster.

IV. CONCLUSION

Using adaptive overlapped segmentation and feature-point matching copy-move forgeries can be detected effectively. The Adaptive Overlapped Segmentation algorithm is to divide the image into non-overlapping and irregular segments adaptively. This will enhance the accuracy of the forgery detection results. Then, in each segments, the feature points are extracted using SURF algorithm it will reduce the computational cost. And the extracted features are matched with one another to locate suspected forgery regions. Afterwards, merged regions are generated and then morphological operation is applied to it to generate the detected forgery regions. This scheme will give forgery detection results faster with a better accuracy under various conditions, such as geometric transforms and JPEG compression compared to the existing systems.

REFERENCES

[1] Chi-Man Pun, Xiao-Chen Yuan, Member, and Xiu-Li Bi," Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching", IEEE Transactions On Information Forensics And Security, vol. 10, no. 8, Aug. 2016
[2] Mahdian and S. Saic,"Detection of copy move forgery using a method based on blur moment invariants", Forensic Sci. Int., vol. 171, nos. 23, pp. 180189, 2007.
[3] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, "Fast and robust forensics for image region-duplication forgery", Acta Automat. Sinica, vol. 35, no. 12, pp. 14881495, 2009
[4] Mohamadian, Z., & Pouyan, A. A. "Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions". Paper presented at the UKSim, 2013.
[5] Alin C. Popescu and Hany Farid."Exposing Digital Forgeries in Color Filter Array Interpolated Images",IEEE Transactions On Signal Processing, Vol. 53, No. 10, Oct 2005.
[6] Ting, Z., & Rang-ding, W. (2009). "Copy-move forgery detection based on SVD in digital image", Paper presented at the Image and Signal Processing, 2009.
[7] Bashar, M., Noda, K., Ohnishi, N., & Mori, K, "Exploring duplicated regions in natural images", IEEE Transactions on Image Processing,(99), 1, 2010.
[8] Zimba, M., & Xingming, S, "DWT-PCA(EVD) Based Copy-move Image Forgery Detection", International Journal of Digital Content Technology and its Applications, 2011.
[9] Luo,W., Huang, J., & Qiu, G, "Robust detection of region-duplication forgery in digital image", Paper presented at the Pattern Recognition ICPR , 2006.
[10] Wang, J., Liu, G., Li, H., Dai, Y., & Wang, Z, "Detection of image region duplication forgery using model with circle block", Paper presented at the Multimedia Information Networking and Security, 2009.
[11] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling", in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2011.
[12] Lin, H.-J., Wang, C.-W., & Kao, Y.-T, "Fast copy-move forgery detection". WSEAS Transactions on Signal Processing, 2009.
[13] Bo, X., Junwen, W., Guangjie, L., & Yuewei, D, "Image copy-move forgery detection based on SURF". International Conference on Multimedia Information Networking and Security (MINES), 2010.
[14] Zheng, J., Haoa,W., & Zhub,W, "Detection of Copy-move Forgery Based on Keypoints Positional Relationship". Journal of Information and Computational Science, 2012.
[15] Nazeema, B.Ramesh Reddy, P.Rakesh Kumar," Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching",IJIRT, vol.3, Sep.2016.
[16] Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copymove forgery detection approaches, IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 18411854, Dec. 2012.