International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

A Novel Integrated Technique for Forgery Detection for Copy-Move Forgery

K.Madhavi[1], D. ManjithKumar[2], S. Mahitha[3]

Assistant Professor, Electronics and communication Engineering (EC) St. martin's Engineering College Secunderabad, India,
Electronics and communication Engineering (EC) St. martin's Engineering College Secunderabd, India.

Abstract: *This paper introduces to image forgery detection by adaptive over segmentation and feature point matching. The proposed method uses both block based and key-point based techniques to detect forgery region. The adaptive over segmentation technique divides the host image or input image into non-overlapping irregular shapes called as image blocks (IB).Then by using the scale invariant feature transform(SIFT)we extract the block features(BF) in each block of the image, following by adaptive block feature matching where the block features of each block are matched or compared with other blocks by this estimated or suspected forgery region can be identified. Then by using forgery region extraction algorithm we convert the labelled feature points are converted into small super pixels and by merging the similar neighbouring feature points and then by using morphological operation we find the forgery region of an image.*

Keywords: *Adaptive over-segmentation, image blocks, SIFT, and block features.*

I. INTRODUCTION

Now a days as technology evolves many techniques and software(s) are developed by the people as per there requirement by this the image editing software(s) are also increased vastly and made available to everyone for free of cost. Using these software(s) we can edit the picture as per our requirement. Due to this there are two types of causes bright side and dark side. The dark side is causing the human life itself. By using these editing tools which are available in the market the image originality can be changed tremendously. This type of work is called as image tampering.

There are many types of image tampering but most and widely used us copy-move tampering which means the one or some part(s) of the image are copied and pasted in the same image or original image because of this method some important factors gets eliminated or compatible such as noise, color components with the original image. Because of this techniques which are based on above factors can't be helped to find the forgery region so the proposed based which uses the image features of the same image can be used to extract the forgery region easily and accurately.

Fig 1: Forged test image "Jeep" (above) and its original version (below).

II. LITERATURE SURVEY

Amruta Jagtap et al [1] this paper proposes that copy-move tampering of an image can be found without prior knowledge of that image by integrating the block based and key point methods. In which the host image is segmented into non-overlapping irregular blocks called as image blocks which are used by the block feature extraction algorithm to extract the feature of each block called block features(BF).Then by applying block feature matching algorithm the block features are compared with each other and labeled feature points(LFP) are found this method finds the almost suspected forgery region to find the forgery region more accurately we propose this method called adaptive feature extraction algorithm where the LFP are converted into small super pixels and are combined with the other feature points which are having same color features called feature blocks then by applying the morphological operations to the merged regions to detect the forgery region.

A. J. Fridrich,[2] this paper is based on exiting method to detect the forgery region which is block –based method. In this method the host image is divided into overlapping

rectangular regular shapes after this the feature points are extracted of each block and compared with the remaining block features this method is efficient for only some extent because the comparison between the blocks takes so much time , becomes computationally expensive if the image size increases and the image can't undergo geometrical transformation of the forgery regions[1].

Devanshi Chauhana[3] this paper proposed the existing method which is used in the proposed method called key-point method.

This method is mainly used to extract the feature points of the host image using SIFT,SURF,MIFT methods. SURF method normally use normal pixel sizes and can detect geometrical transformation like scaling, rotation or transformations performed after forgery. SURF use block based method which has high computational complexity. SIFT is an efficient technique and can detect forgery in a single or multiple regions of an image. Also it is considered to give good detection results in case of both plain copy-move forgery and geometric transformation like scaling, rotation, translation. But SIFT is invariant to rotation, scaling and affine transformation. And SIFT give high computational efficiency compared to SURF. But SIFT accuracy is low compared to SURF.

III PROPOSED METHOD

The proposed method integrates both block based and key-point forgery detection methods. The process is shown in the form of flowchart in figure (1).

a. Adaptive over-segmentation Algorithm:

The Adaptive Over-Segmentation calculation, which is like when the extent of the host pictures expands, the coordinating calculation of the covering pieces will be significantly more costly. To address these issues, we proposed the Adaptive Over-division strategy, which can section the host picture into non-covering districts of unpredictable shape as picture squares thereafter, the fraud areas can be distinguished by coordinating those non-covering and sporadic locales.

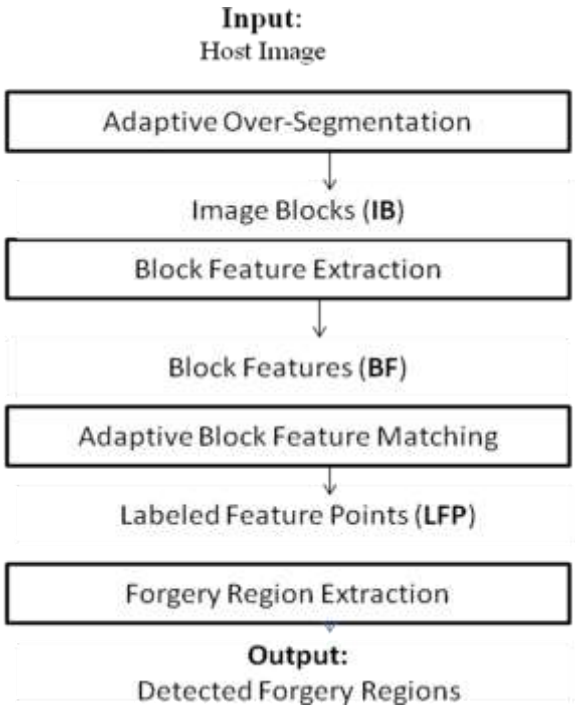


Fig2: Framework of the Proposed Copy-Move Forgery Detection Scheme.

Division strategy, the non-covering division can diminish the computational costs contrasted and the covering blocking; besides, much of the time, the sporadic and important areas can speak to the fraud locale superior to the consistent pieces. Nonetheless, the underlying size of the super pixels in SLIC is hard to choose.

In reasonable utilizations of duplicate move falsification recognition, the host pictures and the duplicate move districts are of various sizes and have diverse substance, and in our fabrication identification strategy, distinctive introductory sizes of the super pixels can create distinctive imitation location comes about; subsequently, unique host pictures ought to be obstructed into super pixels of various beginning sizes, which is exceptionally identified with the phony discovery comes about. We have played out countless to look for the connection between the recurrence circulation of the host pictures and the underlying size of the super pixels to acquire great fabrication identification comes about. We played out a four-level DWT, utilizing the 'Haar' wavelet, on the host picture; at that point, the low-recurrence vitality ELF and high-recurrence vitality EHF can be computed utilizing (1) and (2), separately. With the low-recurrence vitality ELF and high-recurrence vitality EHF , we can compute the level of the low-recurrence conveyance PLF utilizing (3), as indicated by which the underlying size S of the super pixels can be characterized as in (4),

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

$$E_{HF} = \sum_{i} \left(\sum |CD_i| + \sum |CH_i| + \sum |CV_i| \right), i = 1,2,\ldots,4 \quad (2)$$

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}} .100\% \quad (3)$$

$$S = \begin{cases} \sqrt{0.02 \times M \times N P_{LF}} > 50\% \\ \sqrt{0.01 \times M \times N P_{LF}} \leq 50\% \end{cases} \quad (4)$$

Wherein, S will provide us the preliminary size of the super pixels; as well as the scale M × N indicates the size of the host photograph; and P LF approach the share of the low-frequency distribution

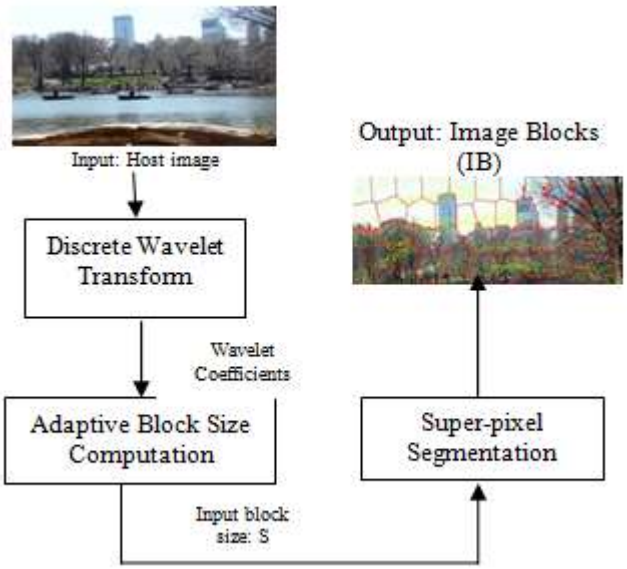


Fig3: Flowchart of adaptive over-segmentation

b. Block feature extraction Algorithm:

After the host picture is divided into picture squares, piece highlights are removed from the picture squares (IB). The customary square based imitation discovery techniques removed highlights of an indistinguishable length from the piece highlights or straightforwardly utilized the pixels of the picture hinder as the piece highlights. In any case, these features reflect generally the substance of the photo pieces, overlooking the range information. Moreover, these features are not impenetrable to various picture changes. Appropriately, in this wander, the component centers are expelled from each photo hinder as square features and the segment centers should be intense to various curves, for instance, picture scaling, insurgency, and JPEG weight. The part point extraction systems, SIFT and SURF have been extensively used. The segment centers made using these

strategies are healthy against essential picture getting ready operations, for instance, turn, scale, darkening, and weight

c. Block feature matching Algorithm:

In the greater part of the current piece based strategies, the square coordinating procedure yields a particular piece combine just if there are numerous other coordinating sets in the same shared position, expecting that they have a similar move vector. At the point when the move vector surpasses a client determined limit, the coordinated hinders that added to that particular move vector are distinguished as areas that may have been replicated and moved. In our calculation, in light of the fact that the piece highlight is made out of an arrangement of highlight focuses, we proposed an alternate strategy to find the coordinated squares.

Algorithm: Block Feature Matching algorithm

Input: Input is Block Features (BF) which is output adaptive over segmentation;

Output: Output is Labeled Feature Points (LFP) which may be suspected region.

STEP-1: First I need to Load the Block capabilities BF =BF1, BF2, ,BFN....., with given N as the number of photograph blocks; remedy it for the correlation coefficients CC of the photo blocks.

STEP-2: Getting the block matching threshold TRB as according to the distribution of correlation coefficients.

STEP-three: supply the place of the matched blocks MB primarily based on the block matching threshold B TR.

STEP-4: From given Label the matched function factors within the matched blocks MB to suggest the suspected forgery regions.

d. Forgery region extraction Algorithm*:*

Once the named highlight focuses (LFP) are separated, there is a need to find the imitation locales moreover. Since, this separated LFP's are just the areas of the phony locales. A Forgery Region Extraction calculation is utilized to distinguish the fashioned areas all the more precisely. To acquire the speculated locales (SR), a strategy by supplanting the LFP with the little super pixels is proposed. This is finished by sectioning the host picture extremely well as small super pixels. The nearby shading highlights of the super-pixels that are neighbors of the presumed At the point when this nearby shading highlight is same as that of the speculated locales, at that point the neighbor super pixels are converged into the comparing presumed districts. This consolidating procedure brings about blended districts (MR). At last, to produce the distinguished duplicate move falsification districts, morphological operation is connected to this consolidated area. Fig.3 demonstrates the flowchart of the Forgery Region Extraction Algorithm

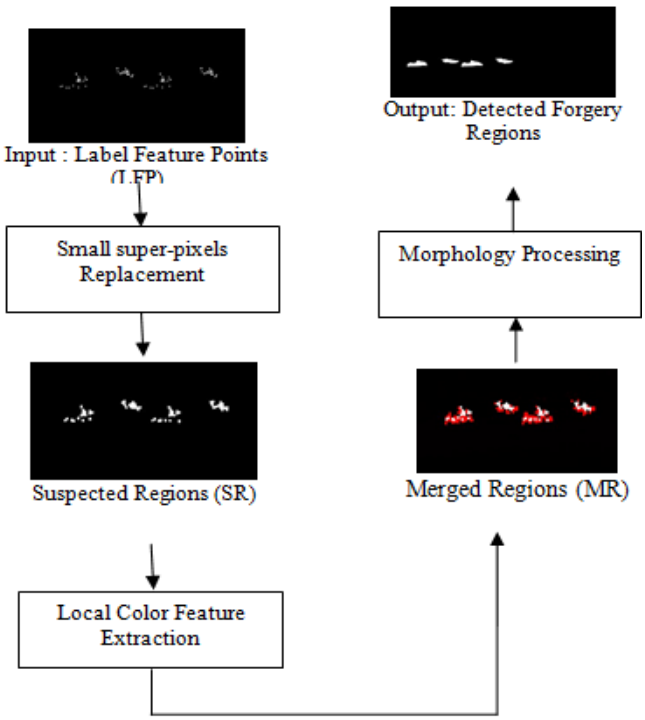


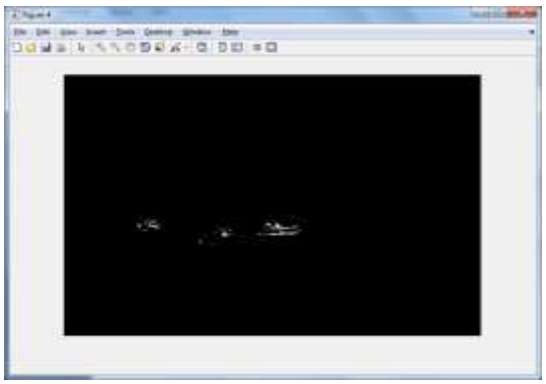
Fig4: Flowchart of forgery region extraction algorithm

IV RESULTS

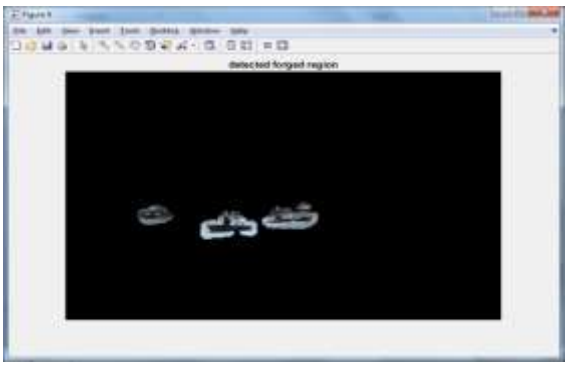
(a):Host image

(b):Forgered image

(c)Image blocks



(d): Labelled feature points



(e):Detected forgery region

Final detected forgered region

Fig 4: Simulation results

The fig (a)&(b) shows the host image or the original image and the morphed or forgery image ,this image will be divided into image blocks using adaptive over-segmentation as shown in figure (c) then the feature points where extracted using the SIFT method and the feature points are matched with each other and then the labeled feature points where extracted and the suspected forgery region is found in the image after that by converting the LFP into small super pixels and then merging the pixels which are having same color components and then by performing the morphological operations the final forgery regions are detected as shown in figures (d)(e)(f).

V. CONCLUSION

In this paper we concluded that the digital images and documents should be properly authenticated from the forgery due to the availability of different software's and tools. So to keep the digital media safe or to detect the forgery region we initially have to divide the image into blocks and then detecting the features in the image comparing them with each other and then the suspected region feature points are converted into

super pixels based on the same color components they are merged together to know the final forgery detected region more accurately. Hence the final forgery image has been detected.

REFERENCES

[1] "Survey Paper on Advanced Techniques for Image Forgery Detection",by Amruta Jagtap, H. A. Hingoliwala, International Journal of Science and Research (IJSR), Vol 4 Issue 12, 2015.

[2] "Detection of copy-move forgery in digital images,"by A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, 2003.

[3] "Survey On Keypoint Based Copy-move Forgery Detection Methods On Image", Devanshi Chauhana *, Dipali Kasatb , Sanjeev Jainc , Vilas Thakare ELSEVIER-2016.

[4] "An evaluation of popular copy-move forgery detection approaches." Christlein, Vincent, et al. , IET, 2012.

[5] "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Points Matching." Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. , IEEE, 2015.

[6] " a Jessica Fridrich, b David Soukal, and a Jan Lukáš", Jessica Fridrich, b David Soukal, and a Jan Lukáš

[7] "Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine"., Musaed Alhussein

[8] "Centroidal Distance Based Offline Signature Recognition Using Global and Local Features", Mr. Raskar Rahul Bhausaheb , Prof. Sandeep Kumar, Mr. Kharade Sachin, Vol 3, Issue 3, 2015.

[9] "Detecting Video Sequence Matching Using Segmentation Method", K.Girija, S.Herman Jeeva, M.Soniya, P.Sabarinathan, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, 2014.

[10] "Detecting Copy–Move Forgeries in Scanned Text Documents" Svetlana Abramova,

[11] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding, 2010, pp. 51-65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," Ieee Transactions on Information Forensics and Security, vol. 8, pp. 1355-1370, Aug 2013.

[13] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, 2011, pp. 1880-1883.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, 2008, pp. 272-276.

[15] X. Y. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," Ieee Transactions on Information Forensics and Security, vol. 5, pp. 857-867, Dec 2010.

[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.

[17] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010, pp. 889-892.

[18] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1018-1028, 2012.

[19] B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSI International Journal of Computer Science Issues, vol. 8, 2011.

[20] D. G. Lowe, "Object recognition from local scale-invariant features," in Computer vision, 1999. The proceedings of the seventh IEEE international conference on, 1999, pp. 1150-1157.

[21] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in Computer Vision–ECCV 2006, ed: Springer, 2006, pp. 404-417.

[22] 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, Dec 2012