International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Advanced Image Forgery Localization Using Labeled Feature Points Extraction

[1]A.Navya Sai Sri , [2]S.Spandana, [3] K.Lakshmi Prasanna, [4] M.Mallika Bhavani, [5] K.Vineetha, [6] N.Rakesh
Department of E.C.E , Tirumala Engineering College , Jonnalagadda-522606.
[1]Nshree6606@gmail.com , [2]sspandana2017@gmail.com, [3]Kunchala.lakshmiprasanna72@gmail.com,
[4]saimallika331@gmail.com , [5]vineethasam28@gmail.com [6]rakeshnalabothu8@gmail.com

Abstract: Basically, different forensic approaches are integrated to obtain good localization performance. But many problems are not studied in the existed forensic approach and this cannot detect the good performance results. In this paper, we propose a framework to improve the performance of forgery localization via integrating tampering possibility maps. In the proposed framework, we first select and improve two existing forensic approaches, i.e., statistical feature-based detector and copy-move forgery detector, and then adjust their results to obtain tampering possibility maps. After investigating the properties of possibility maps and comparing various fusion schemes, we finally propose a simple yet very effective strategy to integrate the tampering possibility maps to obtain the final localization results.

Key Words: Forgery, forgery extraction, detectors, image forensics, transform coding.

1. INTRODUCTION

With the help of powerful image editing software, we can easily modify digital images without leaving any perceptible artifacts. Maliciously tampered images would lead to some potentially serious consequences in our daily life. In this way, image forgery detection has pulled in impressive consideration during the previous decade. For most measurable techniques, it is expected that some image forgery insights presented by the age pipeline will be unavoidably twisted after some altering tasks, and scientists investigate such insights in order to recognize the fabrications. By and large, there are two primary issues in forgery detection, one is fabrication recognition, and the other one is falsification confine Forgery detection expects to serge whether a given picture is perfect or phony. For instance, by exploiting some camera-related signals such as sensor pattern noise (SPN) and color filter array (CFA) properties, it is possible to reveal tampered images via camera source identification [1]. By analyzing the JPEG compression artifacts, one can expose JPEG decompressed images and detect JPEG recompressed images. Based on the distinctive artifacts left by a certain operation, it can identify contrast enhancement reveal image resembling detect median filtering and so on. In practice, a key influential factor for forgery detection performance is the variety and uncertainty of tampering operations. Since most existing forensic methods assume that only one specific tampering operation is under investigation, they should not be used for a real forensic scenario independently. Usually, it requires to analyzing the image with several forensic detectors and combining the detection results using some fusion schemes [2].

In forgery detection, the key idea is that suitable features can capture the deviations from the normal behavior induced by typical image forgeries, such as copy-moves or splicing. It is worth underlining that these deviations are often not perceivable by a human being, since modern image editing tools, if used with proper skill, allow one to manipulate images leaving little or no obvious artifacts, smoothing the boundary between host image and forgery to avoid abrupt transitions It is worth underlining that these deviations are often not perceivable by a human being, since modern image editing tools, if used with proper skill, allow one to manipulate images leaving little or no obvious artifacts, smoothing the boundary between host image and forgery to avoid abrupt transitions. Major efforts have been devoted to find good statistical models for natural images in order to select the features that guarantee the highest discriminative power. Frequently, so as to catch progressively significant measurements, change area highlights have been utilized, where the picture experiences square insightful discrete cosine transform (DCT) with different square sizes and first-request (histogram based) and higher-request (change probabilities) highlights are gathered and combined [3]. Recently, following an approach used in steganalysis, we proposed powerful descriptor-based forgery detection technique.

As we know that the digital image forgery is easily performed by using the computer technology and

image processing software. But in present generation the reliability of digital images is an important issue and many of the researches focused on the problem of digital image tampering. In the existed system this image tampering is manipulated as forgery image localization. This forgery image localization is nothing but to paste one or a few replicated district of a picture into other piece of a similar picture. While playing out the duplicate and move tasks, a portion of the picture preparing techniques like turn, scaling, obscuring, pressure and commotion expansion are connected to the forgeries [4-5].

After the process of copy and move operations some of the properties like noise component, color character and others become compatible to the remainder of the image. Earlier many methods are introduced for forgery detection and the existed system divides the forgery detection into two ways they are statically feature and copy move based approach. Here the existed system will divide the input images into two blocks they are overlapping and regular image blocks. The tampered region is formed by matching blocks of image pixels. This is about the existed system coming to the proposed forgery localized method system, the input is divided into overlapping rectangular blocks. Here to find the tampered regions some of the discrete transform coefficients are matched with each other. To decrease the feature dimensions in proposed system principal component analysis is applied.

In this paper, we propose an improved framework to deal with the problem of image forgery localization. The proposed framework first analyzes the input image using a statistical feature based detector and a copy-move forgery detector, respectively. The results of the two approaches are then converted into tampering possibility maps. By analyzing the properties of tampering possibility maps, we employ a simple yet very effective strategy to obtain the localization result. Compared with the existing methods the main contribution of this paper is to propose a fusion scheme based on tampering possibility maps. The main efforts in our work are as follows. Firstly, after analyzing the most popular tampering operations (splicing/erasing and copy-move) in real cases, we choose two forensic approaches and improve them for forgery localization. Although fewer forensic approaches are utilized compared to existing methods, we still significantly boost the overall performance.

Secondly, unlike the existing methods that use binary maps, we convert the results of the adopted approaches into maps with continuous values ranging from 0 to 1, which indicate the tampering possibilities of the corresponding pixels. In this way, we can preserve more useful intermediate information of each approach and predict whether a pixel is pristine or fake more reliably. Compared to the binary maps, the tampering possibility maps are able to reduce the false positives and false negatives significantly based on our experiments. Finally and more importantly, the fusion method for integrating tampering possibility maps is newly designed.

By analyzing the properties of tampering possibility maps, we integrate the two tampering possibility maps with a carefully designed decision curve, which can more or less keep the advantages of both approaches and make them complement each other for forgery localization.

2. RELATED WORK

In practical forensic applications, we are progressively keen on making sense of the altered locales contrasted with forgery detection identification. In this manner, image forensic turns into a vital issue in picture legal sciences. Since imitation confinement requires pixel-level investigation as opposed to picture level examination, it faces more difficulties contrasted with fabrication identification. As of late, some fraud limitation works have been proposed dependent on JPEG highlights irregularity of photograph reaction non-consistency (PRNU) nearby descriptors, etc.

A substantial number of strategies have been proposed in recent years for forgery detection and localization. Most of them look for traces of image tampering, whatever their nature, as hints of possible image manipulation. Much work has been devoted to copy-moves, obtaining a pretty good accuracy with sparse descriptors, and much better when more complex dense descriptors are used. Splicings, however, are certainly harder to detect than copy-moves. Much of the current literature aims to explore some specific types of processing the forgery could have been subject to. Some methods are based on the artifacts caused by JPEG compress, others on blur inconsistency.

On revealing traces caused by re-sampling, which is a necessary operation whenever the forgery needs to be rotated or rescaled by a certain factor. Substantially more broad strategies are those dependent on camera ancient rarities since they don't make explicit presumptions on the sort of falsification, however exploit some unconventional qualities of the camera under investigation. They are based, for example, on the analysis of color filter arrays and interpolation filters, on artifacts caused by demosaicking, or on the absence of the specific sensor noise (PRNU) that characterizes each camera. Rather than considering camera artifacts, some researchers rely on the statistics which characterize pristine natural images. Regions that have been subject to some kind of

processing are then detected based on the deviation from these statistics. a feature-based procedure is outlined in order to tell apart regions subject to median filtering from region treated by other forms of processing. An analogous approach is used, where a no causal Markov model is considered in order to capture the underlying statistical characteristics of the signal.

Feature-based classification and localization is also performed, where blurring is detected by using features already considered for the evaluation of natural image statistics in the context of image quality assessment. The key idea is that these statistics change when blurring takes place. In all these techniques a two-class (pristine/forged) training procedure is necessary and each method focuses on a particular type of manipulation. The method proposed in this work is itself feature-based, but is not tailored to a specific type of tampering and requires training only on pristine image .

3. EXISTING SYSTEM

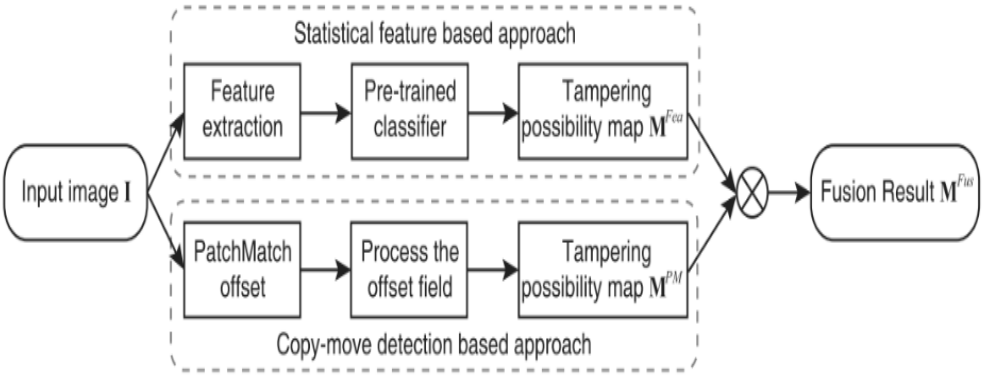

Fig 1: EXISTING SYSTEM

The above figure (1) shows the architecture of existed system. Basically, it is easy to create the copy move forgery. In the same way the source and target regions are obtained from the same image. The main intent of this system is to use copy move detection technique and the image is compressed by using the compressing algorithm that is JPEG. we use two types of methods for forgery copy move detection they are block based method and key point based method. From below figure (1) we can observe the methods of copy move forgery detection. Here in the square based technique the picture is separated into covering squares with particular size and featured vectors are computed on this method. Next one is key point based method; in this the featured vectors are computed with high entropy. To find the copied blocks in this system they used to match the featured vectors.

Up to now we have discussed about the concept of copy mover forgery. Now let us discuss about the detections of copy move forgery detection. Here the copy move forgery will provides the correlation between the original image segment and pasted image segment. This correlation will give the successful detection of the forgery**.** this forgery will saved in an particular format that is lossey JPEG format. But by using the image processing tool the segment may not match exactly but it match approximately. Now let us discuss about the two detection methods which are given below and in the same way these detection algorithm must allow the following requirements, they are The discovery calculation must take into account a surmised match of little picture portion, It must work in a sensible time while presenting couple of false positives, Another characteristic supposition that ought to be acknowledged is that the produced fragment will probably be an associated segment rather than a gathering of exceptionally little fixes or individual pixels.

a) Statistical Feature Based Approach

In this section first the algorithm is used for the purpose of identifying the segments in the image which matches exactly. But this tool is applied in a limited way for forensic analysis. Basically, the user specifies a particular size of an segment for the purpose of matching. Let us discuss this with an example, if the segment is having square of B×B pixels. Presently the square comprises of pixel in the picture from the upper left corner right and down to the lower right corner. Presently in the situation of B×B obstruct the pixel esteem is removed from the sections into a line of a two-dimensional array A with B2 segments and (M– B+1)(N– B+1) columns. Now to find the identical rows the rows of the matrix A are

lexicographically ordered. Thus the lines that are coordinated are effectively sought by experiencing all MN columns of ordered Matrix.

b) Detection Of Copy-Move Forgery By Key Point Method

Coming to the key point based method the input is divided into corner points which provides the Local feature description of an image. Here the detection of key point based copy move forgery is done by extracting high entropy regions. To detect the matched key points and forgery, feature descriptors are matched with each other. In this we use SIFT and SURF as key point descriptors. To detect the copy move forgery region matched descriptors are used and SIFT key point descriptor is extracted. The main intent of this SIFT is to locate the matched key point with rotating and scaling. From below figure (3) we can observe the process of involved in this method. After the process of matching and extracting, the object recognition will be done. SIFT is used in panorama switching for a fully automated Panorama reconstruction from non-panoramic images. But it does not gives better results, to overcome this a new system is proposed which is discussed below.

.

4. PROPSED SYSTEM

The below figure (2) shows the block diagram of proposed forgery detection. In this proposed system the detection process is done by using adaptive over-segmentation and feature point matching methods. Here the main intent of the Adaptive Over-Segmentation strategy is to portion the host picture into Non-covering and irregular blocks. These blocks are known as image blocks. The block features are coordinated with each other and coming to include focuses, these are superbly coordinated with each other and decide the Labeled Feature Points (LFP). This name highlighted focuses speak to the speculated fraud districts. Finally Forgery Region Extraction technique is proposed to identify the imitation area from the host picture as indicated by the removed LFP. Presently given us a chance to examine in insight concerning the adaptive over-segmentation algorithm, block feature algorithm, block Extraction Algorithm and forgery Extraction Algorithm. From this we can say that proposed system gives better result compared to existed system. Let us discuss in detail manner about this system

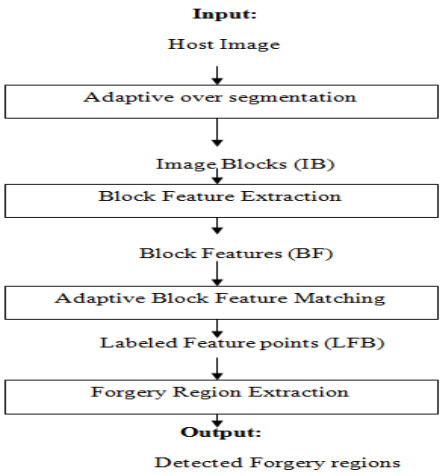

Fig 2: PROPOSED SYSTEM

A. Adaptive Over-Segmentation Algorithm

The main intent of using the adaptive over-segmentation algorithm in copy move forgery detection is that it divides the host image into blocks. As discussed earlier that the block based forgery detection algorithm is proposed where the host picture is separated into covering customary squares with settled size. By coordinating those obstructs the falsification districts are recognized. Hence the detected regions consist of regular blocks and in the same way the recall rate of block based method becomes very low. Here when the size of the host images increases then the matching computation of the overlapping blocks will be much more expensive. To overcome this problem an adaptive over-segmentation algorithm is proposed.

B. Block Feature Extraction Algorithm

In this algorithm we are going to extract the block features from the image blocks (IB). At present we are separating the element focuses from each picture hinder as square highlights, and in different twists these component focuses acts like vigorous like picture scaling, turn, and JPEG pressure. In the key

point-based duplicate move fabrication location strategy we are utilizing SIFT and SURF techniques.

C. Adaptive Block Feature Matching Algorithm

In this algorithm we are going to locate the matched blocks by using block features. But in the existed system it does not give better result. So a different method is proposed to find the coordinated blocks. In this proposed calculation first number of coordinated component focuses is determined and after the computation a connection coefficient Map is created. Finally coordinated component focuses in the coordinated square combines are removed and marked to find the situation of the speculated imitation locale.

D. Forgery Region Extraction Algorithm

The main intent of this algorithm is to locate the forgery regions. This process is done after the extraction of the labeled feature points (LFP) we locate the forgery regions. By using the super pixels the host picture is portioned in a very nice way and also to obtain the suspected regions we will use the super pixels. Now to improve the precision and recall results we measure the local color features of the super-pixels and if the color feature of the suspected regions is same, at that point we blend the neighbor super pixels into the comparing speculated locales.

5. RESULT

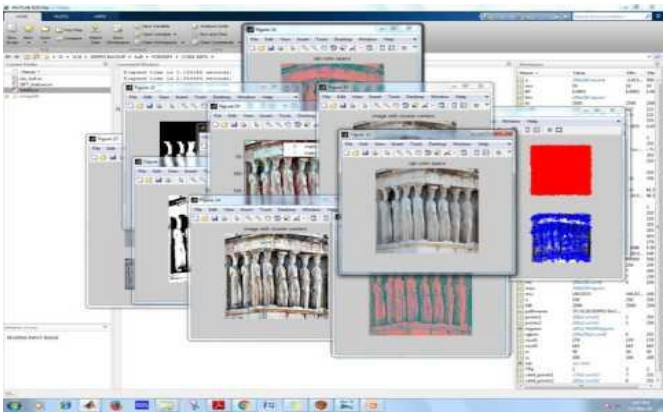

Fig 3:Simulation Output

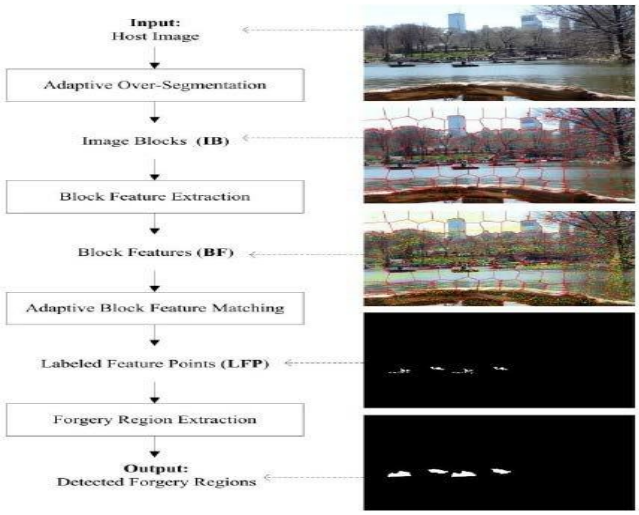

Fig 4: Stage Wise Results

6. CONCLUSION

Basically, to detect the copy move operations a digital forgery images are created. But in this paper we proposed image forgery localization technique using adaptive over-segmentation and feature-point matching methods. The adaptive over segmentation

algorithm fragments the host picture into non covering and sporadic squares and after that the element focuses are separated from each block as block highlights. Here the block highlights are coordinated with each other to find the marked element focuses. From this procedure we can watch the presumed fabrication areas. To distinguish the falsification areas, the forgery region extraction algorithm is proposed by supplanting the component focuses with little super pixels as highlight blocks. After this procedure it combines the neighboring blocks to produce the consolidated areas. Thus it gives better outcomes contrasted with existed framework.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in in Proceedings of Digital Forensic Research Workshop, 2018.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2017.

[3] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, 2016, pp. 746-749.

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Multimedia and Expo, 2007 IEEE International Conference on, 2015, pp. 1750-1753.

[5] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic science international, vol. 171, pp. 180-189, 2014.

[6] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Computer Science and Software Engineering, 2008 International Conference on, 2013, pp. 926-930.

[7] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2012, pp. 1053-1056.

[8] M. Kirchner and J. Fridrich, “On Detection of Median Filtering in Digital Images,” SPIE, Electronic Imaging, Media Forensics and Security XII, vol. 7541, pp. 101–112, jan. 2011.

[9] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, “Determining image origin and integrity using sensor noise,” IEEE Transactions on Information Forensics and Security, vol. 3, no. 1, pp. 74–90, 2010.

[10] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, “An Evaluation of Popular Copy-Move Forgery Detection Approaches,” IEEE Trans. on Information Forensics and Security, vol. 7, no. 6, pp. 1841–1854, 2009