Image Forgery Detection Using Adaptive Over Segmentation and Feature Point Matching

Nazeema[1], B.Ramesh Reddy[2], P.Rakesh Kumar[3]
[1,2,3] *Electronics and communication Engineering, LBRCE, Andhra Pradesh, India*

***Abstract*—a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching is proposed in this paper. The proposed scheme integrates both block-based and key point-based forgery detection methods. First, the proposed Adaptive Over-Segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labelled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the Forgery Region Extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neighbouring blocks that have similar local colour features into the feature blocks to generate the merged regions; finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy-move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy-move forgery detection methods.**

***Index terms*—Copy-Move Forgery Detection, Adaptive over Segmentation, Local Colour Feature, Forgery Region Extraction**

I. INTRODUCTION

We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images. Here I review the state of the art in this new and exciting field. Digital watermarking has been proposed as a means by which an image can be authenticated. The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories: 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post processing.

As the use of images have been increasing day by day in our lives, with the introduction of digital technology, The forgery of digital image has become more and more simple and indiscoverable. Today's digital technology had begun to erode the integrity of images and image counterfeiting and forgeries with the move to the world of Megapixels, opens a new door to the dark-side of it. We are living in an age, where anything can be manipulated or altered with the help of modern technology. With the increasing applications of digital imaging, different types of software tools are introduced for processing images and photographs. They are used to make forge images to make it look real or objects can be added or deleted. For decades, photographs have been used to document and they have used as evidence in courts. But this process is very time consuming and requires expert knowledge so it is hard to implement than digital pictures. Today, however, powerful digital image

editing software makes image modifications straightforward [1]. Today's digital technology has begun to remove trust in our knowledge, as from the magazines, to fashion world and in scientific journals, political campaigns, courts and the photo that come in our e-mail. In all of these forged photographs are appearing with a more frequencies and sophistication. In the increase in the availability of multimedia data in digital form has come to a tremendous growth of tools to manipulate digital multimedia contents. The process of creating fake image has been tremendously simple with the introduction of new and powerful computer graphics editing software which are freely available as Photoshop, GIMP, and Corel Paint Shop. Today, this powerful image processing software's allow people to modify photos and images conveniently and unperceivable. Now days it creates a big challenge to authenticate images. Image forgery means manipulation of the digital image to conceal some meaningful or useful information from it. Sometimes it is difficult to identify the edited region from the original image. The detection of a forged image is driven by the need of authenticity and to maintain integrity of the image. The survey has been done on existing techniques for forged image and it highlights various copy–move detection and splicing detection methods based on their robustness and computational complexity [2].A forgery detection method that exploits subtle inconsistencies in the colour of the illumination of images. To achieve this, we incorporate information from physics- and statistical-based illuminate estimators on image regions. We try to extract texture and edge-based features from the illuminate estimates. These features are provided to a machine-learning approach for making decision automatically. The classification performance using an SVM meta-fusion classifier is promising. A SVM classifier is trained for using statistical features of pattern noise for classifying smaller blocks of an image. SVM classifier is used which have similar functional form to neural networks. Image, texture and pixel value based features are extracted and analyzed from the images. Then has values are calculated for these features. The process consists of two phases, which are training phase, and a testing phase.

II. LITERATURE

Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery [1], which is to paste one or several copied region(s) of an image into other part(s) of the same image. Noise addition is occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, colour character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case. In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms [1-13] and feature key point-based algorithms [14-19].

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Fridrich et al. [1] proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. Popescu and Farid [2] applied Principal Component Analysis (PCA) to reduce the feature dimensions. Luo et al. [3] used the RGB colour components and direction information as block features. Li et al. [4] used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic [5] calculated the 24 Blur-invariant moments as features. Kang and Wei [6] calculated the singular values of a reduced-rank approximation in each block. Bayram et al. [7] used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. [8, 9] used the mean intensities of circles with different radii around the block centre to represent the block features. Lin et al. [10] used the gray average results of each block and its sub-blocks as the block features. Ryu et al. [11, 12] used Zernike moments as block features. Bravo-Solorio and Nandi [13] used information entropy as block features.

As an alternative to the block-based methods, key point-based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In [14-16, 18], the Scale-Invariant Feature Transform

(SIFT) [20] was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In [17, 19], the Speeded up Robust Features (SURF) [21] were applied to extract features instead of SIFT. However, although these methods can locate the matched key points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate [22].

Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Although these algorithms are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases; 2) the methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Although the existing key point-based forgery detection methods can avoid the first two problems, they can reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing key point-based forgery methods were very poor.

III. SUPERPIXEL SEGMENTATION

Super pixels provide a convenient primitive from which to compute local image features. They capture redundancy in the image [1] and greatly reduce the complexity of subsequent image processing tasks. They have proved increasingly useful for applications such as depth estimation [2], image segmentation [3, 4], skeletonization [5], body model estimation [6], and object localization [7]. For super pixels to be useful they must be fast, easy to use, and produce high quality segmentations. Unfortunately, most state-of-the-art super pixel methods do not meet all these requirements. As we will demonstrate, they often suffer from a high computational cost, poor quality segmentation, inconsistent size and shape, or contain multiple difficult-to-tune parameters. The approach we advocate in this work, while strikingly simple, addresses these issues and produces high quality, compact, nearly uniform super pixels more efficiently than state-of-the-art methods [8, 9, 5, 10]. The algorithm we propose, simple linear iterative clustering (SLIC) performs a local clustering of pixels in the 5-D space defined by the L, a, b values of the CIELAB colour space and the x, y pixel coordinates. A novel distance measure enforces compactness and regularity in the super pixel shapes, and seamlessly accommodates greyscale as well as colour images. SLIC is simple to implement and easily applied in practice – the only parameter specifies the desired number of super pixels. Experiments on the Berkeley benchmark dataset [11] show that SLIC is significantly more efficient than competing methods, while producing segmentations of similar or better quality as measured by standard boundary recall and under-segmentation error measures. For many vision tasks, compact and highly uniform super pixels that respect image boundaries, such as those generated by SLIC in Fig. 1, are desirable. For instance, graph-based models such as Conditional Random Fields (CRF) can see dramatic speed increases when switching from pixel-based graphs to super pixels [3, 7], but loose or irregular super pixels can degrade the performance. Local features such as SIFT extracted from the image at super pixel locations become less meaningful and discriminative if the super pixels are loose or irregular, and learning statistics over cliques of two or more super pixels can be unreliable. This effect can be seen when we compare the performance of SLIC super pixels to competing methods for two vision tasks: object class recognition and medical image segmentation. In both cases, our approach results in similar or greater performance at a lower computational cost in comparison to existing methods.

Fig 1 Image segmented using algorithm into super pixels of (approximate) size 64, 256, and 1024 pixels. The super pixels are compact, uniform in size, and adhere well to region boundaries.

A. Scale invariant feature transform

The original SIFT feature detection algorithm developed and pioneered by David Lowe is a four stage process that creates unique and highly descriptive features from an image. These features are designed to be invariant to rotation and are robust to changes in scale, illumination, noise and small changes in viewpoint.

The features can be used to indicate if there is any correspondence between areas within images. Clusters of features from an image that are similar to a cluster of features from another image may indicate, with a high likelihood, areas that match. This allows object recognition to be implemented by comparing features generated from input images to features generated from images of target objects. The four stages of the SIFT algorithm are as follows, full details of which are given in Lowe's paper [11].

1. *Scale-space extrema detection*. The first step is to create a Gaussian scale-space pyramid for the image. Successive blurred images are produced from the convolution of Gaussian functions to create multiple octaves. The difference of Gaussian (DoG) is calculated as the difference between two consecutive images within an octave. The initial set of candidate features are selected by comparing each point in the DoG images to its 26 neighbours and looking for extrema.

2. *Feature localisation*. The number of features is reduced in this stage. Interpolation occurs to locate the exact, sub pixel, location of the candidate features and points that are in areas of low contrast or those that are localised along edges are eliminated.

3. *Orientation assignment.* The image gradient directions of the pixels in a feature's neighbourhood are calculated and added to an orientation histogram with 36 bins. The values in the neighbourhood are Gaussian weighted so those nearer the centre have a greater effect on the resulting orientation. One key orientation is selected for each feature.

4. *Creating the feature descriptor.* The feature descriptor is a 128 dimensional vector which describes the pixel properties of the area surrounding a feature. A 4 by 4 array of 16 histograms is centred on the feature and rotated to match the key orientation calculated in the previous step. The gradient magnitudes are given a Gaussian weighting, added to the histograms and normalised to create the descriptor.

To match features often the Euclidean distance between two feature vectors is used to find the nearest neighbour.

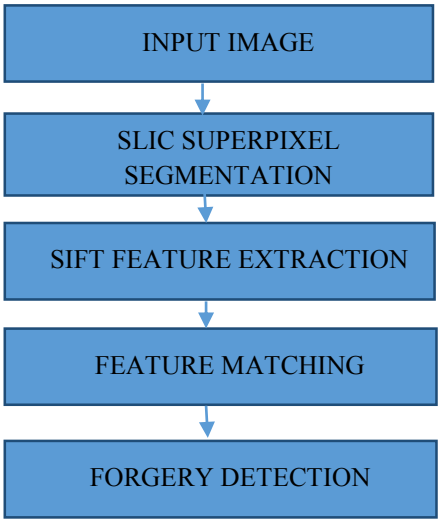

Fig. 2 Framework of the proposed forgery detection scheme

IV. EXPERIMENTAL RESULTS

Fig. 3 Input image

Fig. 4 Forgery Input image

Fig. 5 SLIC segmentation

Fig. 6 SIFT features

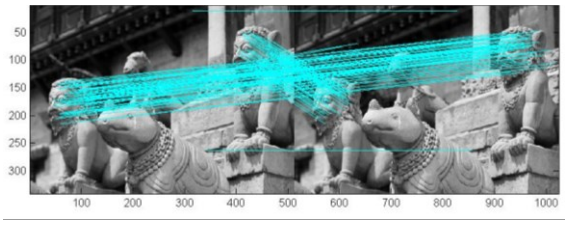

Fig. 7 SIFT matching

Fig. 8 Forged areas

V. CONCLUSION

Digital forgery images created with copy-move operations are challenging to detect. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over-Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses.

REFERENCES

[1] 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, 2003.

[2] C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci.,Dartmouth College, Tech. Rep. TR2004-515, 2004.

[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, 2006, pp. 746-749.

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

[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, 2008, pp. 926-930.

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

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, 2009, pp. 25-29.

[9] J.Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automatica Sinica, vol. 35, pp. 1488-1495, 2009.

[10] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, pp. 188-197, 2009.

[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 Post processed 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.