

Digital Image Forgery Detection

Archa Ajith¹, Bindhu J S²

¹(Department of Computer Science, College of Engineering Perumon, Kollam, India)

²(Department of Computer Science, College of Engineering Perumon, Kollam, India)

Abstract: A forgery detection scheme using feature point matching and adaptive over segmentation is proposed in this paper. Integration of key point based forgery detection methods and block based detection methods are taken place. The adaptive over segmentation algorithm will divide the host image into irregular and non overlapping blocks in an adaptive manner. The feature points are extracted as block features from each block. These block features are then mapped with one another to locate the labeled feature points. This leads to indicate the suspected forgery regions. To detect the forged images in more accurate way, we propose an algorithm called Forgery Region Extraction Algorithm. It replaces the feature points in the image with minimum super pixels as feature blocks. It then performs the merging operation on the neighboring blocks that have similar local features. The merged region is obtained as a result. Forged regions are detected by performing the morphological operation to the merged regions. The result show that proposed detection scheme can achieve better results under certain conditions compared with the existing forgery detection methods.

Keywords: Forgery region extraction, copy move forgery, adaptive over segmentation

I. Introduction

Digital images have a lead role in different technologies and fields. Today manipulation of digital images has become quite easier because of various powerful computers, high resolution capturing devices and advanced photo editing software packages. An image can be easily manipulated which further leads to hiding of useful information or leading to misinterpretations. Duplication performed on these digital images are called forgeries. Such images are called forged images.

Different types of forgeries are present. Copy move forgery, image inpainting etc. These types of manipulations of the images may cause several issues regarding the authenticity, integrity and reliability of the images. In copy move forgery, a certain part of the image is copied and then it is moved to another part of the same image. The image may have several duplications of the same object leading to the forged image. Different Image processing methods like blurring, scaling, rotation, compression and noise addition are also applied to make forgeries. The copy and move parts occur in the same image. So there are certain features like color feature, noise component that are compatible. Hence forgery detection methods based on related image properties are not applied in this case. In previous years many copy move forgery detection methods are available. The aim of the copy move image detection method is to find the duplications which is performed in the images. However, these regions might not be the exact duplicates, since the tamper could use retouching tools, add noise, or compress the resulting image.

Image inpainting is one of the important image duplication method. This technique is used to restore the tampered image. It also leads to the removal of objects from an image. Image inpainting may fill the holes left by object removal through utilizing the nearby or neighboring information. It will preserve the structure continuity and texture. Image inpainting can be exploited to remove image semantic objects for malicious attacks. Here image inpainting becomes a forgery manipulation.

Copy move forgery detection methods is classified into two types: block based algorithms and feature key point based algorithms. These methods are different from each other. They are different in the sense that in block based approach, the host image is divided into various blocks and then the operations are performed. In the case of key point based algorithm, the host image is divided into several blocks and then the features are extracted to detect the forgery image. Different methods may provide different accuracy rate, complexity in calculation and also reduces the time required for the detection.

II. Existing System

In [1], the copy move forgery is detected by using a different method. Comparing to other existing approaches, it is more robust to various image processing methods. The counting bloom filters are used in this cases, which will increase the efficiency by slightly reducing in robustness. Here, the method called lexicographic sorting is used, which determines the similarity of block features.

In [2], the type of forgery or tampering detected is blurred image. The blurred regions are classified into two types. Near Isotropic blur and directional motion blur. The blurred image will reduce the quality of the image. So it should be detected and removed. It is detected by using some transformation methods such as Discrete Wavelet Transform, Discrete Fourier Transform or wavelet transform. It results in lower computational complexity. The method used are invertible and orthogonal. Automatic post processing is introduced. But it is expensive. It will reduce the quality of the picture. As a result the quality cannot be assured.

In [3], the duplicated region or object in a digital image is detected by applying Principal Component Analysis to the fixed size image blocks. The size of the block is not adaptive. It will yield a reduced dimension representation. Lexicographical sorting is also incorporated. The principal component analysis may capture the discriminating features better than the lexicographic sorting. But this method has a drawback that, it is sensitive to small variations between the duplicated regions due to lossy compression or additive noise. Detection results are nearly perfect. But in case of small block sizes, it may not be the case. Accuracy is not good for small block sizes.

In [4], the method used to detect the forgery image is SURF. The multidimensional data matching is performing using KD tree. SURF is Speed Up Robust Feature. It has a detector and descriptor, which is faster and at the same time it is robust to various photometric deformations. KD is used for key point matching, which produces reliable results than lexicographic sorting. Images with high resolution can be used for detection. Duplicated regions with different size can be detected. A few small copied regions may not successfully detected.

In [5], Zernike moments are used for the detection method. It is used to localize the duplicated regions. It is used to detect the copy rotate move forgery ie the CRM forgery. So in order to provide spatial synchronization between the duplicated region and the neighboring regions, geometrical modification like rotation is used. The magnitude of Zernike moments are used to detect the rotated forged region. It performs well even when the noises like Gaussian noise is added. Several detection errors also occurred due to Quantization. So this method is weaker when scaling occurs.

In [6], it uses a super pixel algorithm, that is, the SLIC algorithm, which is used to generate the super pixels. The super pixels are the atomic regions, which is used to perform the segmentation method. It adapts the K-means clustering approach. This simple linear iterative clustering algorithm adheres to boundaries. It is memory efficient method and faster method. Existing super pixel methods are graph based or gradient ascent method. It will reduce the calculation and computational complexity. But the disadvantage is that it do not consider the information regarding the colour. Hence, it may adversely affect the performance of detection.

In [7], it proposed a method which is used to obtain the 1D descriptor which is an invariant to rotation and reflection. The pixels are re-sampled. As a result, log-polar coordinates are obtained and then it is summed to obtain the descriptor. Efficient searching of similar blocks in the forged area is performed using this approach. It is used to overcome the synchronization problems which is caused by geometric transformations. It detect the copied region more properly. It decreases the false positive

In [8], it proposed a square block matching technique. The original image is divided into chunks which is overlapping. A local binary pattern texture method is used for extracting the block features. Gray scale conversion of image is applied to the input image. Lexicographical sorting is used in these blocks. Then for the identification of the duplicated blocks the similarity criterion is used. This method is robust to rotation and flipping. But the defect is that when a region is rotated by general angles it is difficult to detect the forgeries.

In [9], it is proposed to obtain the transformation parameters. It detect the occurrence of copy move tampering. Scale Invariant Feature Transform (SIFT) is used to describe the points or pixels which is present in the forged area. This technique also works well against the splicing attacks ie splicing of an image into a different image. It is used for fingerprint detection and shoe print image retrieval. It provides reliability. It gives reliable estimates. Hierarchical clustering is used.

In [10], it proposed an algorithm to detect an image in the case of Gaussian blurring & JPEG compression. The main goal is to ensure the authenticity and the integrity of image. Single value decomposition and projection data is used to propose an algorithm which is developed based on an expanding block. It provides stronger robustness and it detects the multiple forgeries. It is more precise. SVD has properties ie the stability, rotation invariance and stability. It reduces noises. It used less features and uses more effective.

III. Proposed System

The proposed approach uses adaptive over segmentation and feature point matching technique. These methods help to reduce the drawbacks of the existing system. In the existing system, the size of the superpixel is fixed already. It might not detect the results with higher accuracy. The detected forged area will not be accurate. The miss probability will be higher. The adaptive over segmentation method will divide the host image into various blocks of adaptive size. These image blocks are then subjected to feature point matching.

Host image is given as input to the adaptive over segmentation. Simple linear iterative clustering is used for segmentation method. Image blocks then obtained will be given to the block feature extraction method. DWT is applied to extract various frequency distributions of the host image. The SIFT method is used for block matching. This frequency distribution is used to determine the block size initially. Labelled feature points are obtained as a result. The suspected forgery region is represented by using this LFP. The LFP are then subjected to the forgery region extraction algorithm.

IV. Conclusion

Tampered digital images are difficult to identify. Now a days several editing tools are available, which is cheaper. So various types of duplications are available which is difficult to detect. These duplicated images have bad impact in our society. So we need to detect these types of forged images. Here, a forgery detection scheme using feature point matching and adaptive over segmentation is introduced. The image is segmented into non overlapping segments using the adaptive algorithm called adaptive over segmentation algorithm. It will reduce the computational expense. In order to improve the accuracy, the block size is determined initially. In order to locate the Labeled feature points, the feature matching algorithm is proposed. Hence it can provide much better detection result.

References

- [1] S. Baysram, 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*, 2009, pp. 1053-1056.
- [2] 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*, 2007, pp. 1750-1753.
- [3] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*, 2004.
- [4] 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.
- [5] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding*, 2010, pp. 51-65.
- [6] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," *IEEE Trans Pattern Anal Mach Intell*, vol. 34, pp. 2274-82, Nov 2012.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.