INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue4)

Available online at: www.Ijariit.com

Review of Copy Move Forgery with Key Point Features

Mrs.Nisha[1], Mr. Mohit Kumar[2]

nishamarken@gmail.com[1], mrmohitkumar@yahoo.com[2]

Department of Computer Science

ASRA College, Sangrur

Abstract— It involves the following steps: first, establish a Gaussian scale space; second, extract the orientated FAST key points and the ORB features in each scale space; thirdly, revert the coordinates of the orientated FAST key points to the original image and match the ORB features between every two different key points using the hamming distance; finally, remove the false matched key points using the RANSAC algorithm and then detect the resulting copy-move regions. The experimental results indicate that the new algorithm is effective for geometric transformation, such as scaling and rotation, and exhibits high robustness even when an image is distorted by Gaussian blur, Gaussian white noise and JPEG recompression.

Keywords— Copy Forgery, ORB, SIFT, SURF.

I. INTRODUCTION

In the past ten years, image forgery detection has being emerged as a remarkable research in applications of computer vision, digital image processing, biomedical technology, criminal investigation, image forensics, etc. It becomes more attractive and challenging when powerful software tools for image processing are so popular and sophisticated that we cannot confirm whether an image is manipulated by naked eyes[1]. Image forgery detection is one kind of passive techniques using blind algorithms to detect traces of tampering in a given image without prior information or security codes. The images can be forged by splicing details from itself, which is called Copy-Move images, or from the other images called spliced images. For Copy-Move images, copied regions in image can be post processed, rotated/flipped and scaled before pasting to other places to hide or remove any details.

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. An attempt is made to survey the recent developments in the field of digital image forgery detection and complete bibliography is presented on blind methods for forgery detection. Blind or passive methods do not need any explicit priori information about the image. First, various image forgery detection techniques are classified and then its generalized structure is developed. An overview of passive image authentication is presented and the existing blind forgery detection techniques are reviewed. The present status of image forgery detection technique is discussed along with a recommendation for future research.

In order to separate the copying source region from the pasting target region, the image should be segmented into small patches, each of which is semantically independent to the others. This job is best done by an expert with much experience of digital forensics. The set of image forensic tools can be roughly grouped into four 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; 4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light.

1.2 Types of Image forgery

a) Image Retouching: This is considered to be less harmful kind of digital image forgery. Image retouching is not significantly change an image but instead enhance or reduces certain features of images. This technique is popular among magazines photo editors.

b) Image Splicing: This technique is more aggressive than retouching. Image Spicing is a technique that involves a composite of two or more images which are combined to create a fake image.

c) Copy-Move Attack: Copy-Move attack is more similar to image splicing in view of the fact that both techniques modify certain image region with another image. In other words the source of the modified image originated from the same image.

1.3 Forgery Detection

Forgery detection methods become much more complicated to deal with the latest forgery techniques. This back to the availability of digital editing tools, alteration, and manipulation become very easy and as a result forgery detection becomes a complex and threatening problem. Image forgery detection can be manipulated in various ways with many simple operations like affine transforms such as translation, scaling, etc., compensation operations such as brightness, colours, contrast adjustments, etc., suppression operation such as noise extraction, filtering, compression, etc., furthermore, more complex operations are also possible such as compositing, blending, matting, cropping, photomontage leading to visually untraceable artifacts in an image. The automatic and scientific method of detecting the forged images has become a big challenging problem for researchers and the same problem is true for every multimedia contents.

II. LITERATURE REVIEW

Jian Li et al., [2015], proposed propose a scheme to detect the copy-move forgery in an image, mainly by extracting the keypoints for comparison. The main difference to the traditional methods is that the proposed scheme first segments the test image into semantically independent patches prior to key point extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process consists of two stages. In the first stage, we find the suspicious pairs of patches that may contain copy-move forgery regions, and we roughly estimate an affine transform matrix. In the second stage, an Expectation-Maximization- based algorithm is designed to refine the estimated matrix and to confirm the existence of copy move forgery. Experimental results prove the good performance of the proposed scheme via comparing it with the state-of- the-art schemes on the public databases.

Cheng-Shian Lin et al., [2015], have used an efficient scheme for detecting copy-move forgery tampering attacks. The copy-move forgery attack is defined as a region of an image is replaced by a copy of other region in the same image. This detection is useful for malicious modifying an image. The proposed scheme improves previous cluster expanding block scheme to clustering by mean and variance for reducing the computation time. Experimental results show that the proposed scheme requires fewer computation time. Although the overhead of pre-processing is an extra load that takes more time than previous cluster expanding block scheme, but the total computation time is still improved at least 10% comparing with previous study. Moreover, the using of block variance reduces the false positive rate.

Harpreet kaur et al.,[2015], have used two copy-move image forgery detection methods namely ‘SURF’ and ‘PCA combined with SIFT’ have been implemented using MATLAB platform. It has also been observed that the detection accuracy of ‘PCA combined with SIFT’ method is superior to ‘SURF’ and ‘DWT combined with SIFT’ methods. However this method is unable to detect image forgery in flat region considerably.

Hashmi et al., [2013], have used a vector with seven elements to describe the feature of each small blocks, a 9-dimensional vector is also introduced in to solve the problem with a fixed angle rotation on the copied regions. Elements of this vector are calculated based on the intensities from four equal-sized sub-blocks on each block. The first element is the average intensity, the next four elements are ratios of average intensities and the last four elements are differences of average intensities. A radix sort algorithm is applied to perform lexicographical sorting on these vector sand a forgery manipulation is also detected. The rotation with fixed angle can be detected but not with arbitrary angles by this methods.

Hieu Cuong et al., [2012], proposed Radon transformation to extract the features and use phase correlation to detect the pairs of matching vectors. The proposed method is well performed for the forged images which the rotation angle of the copied region is less than 4o, has Gaussian noise addition with a SNR greater than 35dB and smaller block size 8x8 pixels.

Preeti Yadav et al., [2012], introduced an improved algorithm by applying DWT into an image to reduce the dimension representation. The feature vectors will be extracted from the small overlapping blocks of the compressed image and sorted lexicographically to find the duplicated blocks. The detection was carried out on the lowest level image representation and also proved best performance on small size copy move forgery, detected the multiple Copy-Move forgery with lower computational complexity.

Springer [2010], introduced to solve the problem of the false matching and low robustness in detecting copy-move forgeries, a new method was proposed in this study. It involves the following steps: first, establish a Gaussian scale space; second, extract the orientated FAST key points and the ORB features in each scale space; thirdly, revert the coordinates of the orientated FAST key points to the original image and match the ORB features between every two different key points using the hamming distance; finally, remove the false matched key points using the RANSAC algorithm and then detect the resulting copy-move regions. The experimental results indicate that the new algorithm is effective for geometric transformation, such as scaling and rotation, and exhibits high robustness even when an image is distorted by Gaussian blur, Gaussian white noise and JPEG recompression; the new algorithm even has great detection on the type of hiding object forgery.

Amerini et al., [2008], proposed a method based on clustering the matched keypoints ,which was also adopted by the CMFD evaluation framework. This method was further improved in where the clustering object became a vector associated to the candidate transform estimation.

WeiqiLuo et al., [2006] proposed an algorithm to extract image features by using seven characteristics features computed from the statistical analysis of pixels in an image block. The first three features are the average of red, green, and blue components respectively and the other four features are computed based on the division of that block into two parts in4 directions: horizontal, vertical, and two diagonal directions. To obtain the correct matching, the main shift vector which has the highest frequency of occurrence is also defined. It gives low computational complexity and more robust against various post region duplication image processing graphics operations.

H. Farid et al., [2006], proposed to detect the duplication in science images by grouping the pixels with similar properties. However, being designed for the science images such as gel and micrograph, Farid's method is not efficient and robust enough for normal images that are content rich and contain many different textures.

REFERENCES

[1] Jian Li., Xiaolong Li., Bin Yang, and Xingming Sun, (2015), "Segmentation-Based Image Copy- Move forgery Detection Scheme", IEEE Transactions on Information Forensics And Security ,10(3), pp. 507-518.

[2] Cheng-Shian Lin, Chien-Chang Chen, Yi-Cheng Chang, (2015), "An Efficient Enhanced Cluster Expanding Block Algorithm For Copy-Move Forgery Detection", International Conference on Intelligent Networking and Collaborative System, pp. 228-231.

[3] Harpreet Kaur, Joyti Saxena and Sukhjinder Singh, (2015), "Key-point based Copy-Move Forgery Detection and their Hybrid" Journal of the International Association of Advanced Technology and Science, 16(2), pp. 1-7.

[4] Hashmi M. F., Hambrade A. R. and Keskar A.G., (2013), "Copy Move Forgery Detection using DWT and SIFT Features", IEEE 13 th International Conference on Intelligent Systems Design and Applications (ISDA), pp. 188-193.

[5] Hieu Cuong Nguyen and Stefan Katzen beisser, (2012), "Detection of Copy-Move forgery in digital images using Radon transformation and phase correlation", IEEE 18 th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Piraeu, pp. 418-449.

[6] W. Luo, J. Huang and G. Qiu (2006), "Robust detection of region-duplication forgery in digital images", in: International Conference on Pattern Recognition, vol. 4, pp. 746–749.

