ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 5, Special Issue 4, March 2016

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

Detection of Image Region Duplication

Anjana K Saju[1] , Mercy George[2]

PG Student [Advanced Communication & Information Systems], Dept. of ECE, MBITS, Nellimattom, Kerala, India [1]

Assistant Professor, Dept. of ECE, MBITS College, Nellimattom, Kerala, India [2]

ABSTRACT: Understanding a digital image is authentic or not, is a key purpose of image forensics. There are several different tampering attacks but, surely, one of the most common and immediate one is copy-move. Recent and effective approaches for detecting copy-move forgeries is to use local visual features such as SIFT. In this kind of methods, SIFT matching is often followed by a clustering procedure to group keypoints that are spatially close. Often, this procedure could be unsatisfactory, in particular in those cases in which the copied patch contains pixels that are spatially very distant among them, and when the pasted area is near to the original source. In such cases, a better estimation of the cloned area is necessary in order to obtain accurate forgery localization.

KEYWORDS: Digital image forensics, Tampering detection, Copy-move detection,

I. INTRODUCTION

Images have acquired the reputation of being inarguable evidence. However, with the development of imaging technology and the accessibility of powerful affordable image editing tools like Photoshop, the evidence of tampering on digital images is extremely difficult to uncover. As a result, today digital images are losing authenticity and taking their authenticity for granted is becoming increasingly difficult in legal cases, in electronic media, in medical profession, and in financial institutions.

Image splicing and copy-move are the most common techniques used for creating digital image forgeries. In image splicing, forgery is done by copying a part from one image and pasting to another one. On the other hand, in the copy-move, the copied part is pasted elsewhere in the same image to either add or hide objects. Usually, some processing is done on the copied part either before (e.g. scaling and rotation) or after (e.g. blurring and adding noise) pasting to make the editing less obvious and to eliminate irregularities that could show the image as tampered.

II. EXISTING METHOD

A copy move forgery a portion of an image is copied to different location on the same image. It is difficult to distinguish and detect because the copied part has the properties like noise, colour and texture, will be compatible with the rest of the image. One method for detecting the copy-move forgery is by block-matching [1] procedure, which first divides the image into overlapping blocks. It hence detect the image blocks that where duplicated, instead of detecting the whole duplicated region. Since the copied region would consist of many overlapping blocks and moving the region means moving all the blocks by the same amount, the distance between each duplicated pair would be the same. In this way the decision of forgery can be made and detected.

III. FRAMEWORK OF THE PROPOSED METHOD

In our proposed CMFD scheme, after segmenting the image, we perform the first stage of affine estimation. During this stage we first extract the keypoints from the whole image and construct a k-d tree. Then the KNN (k-nearest neighbour) search is performed in each region for each keypoint to find a possible correspondence. One region is recorded if it has a certain proportion of keypoints matched with another one. Finally we estimate the affine relationship between the region pairs.

IMAGE SEGMENTATION

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 [10].. In our implementation, however, we only consider the automatic approach. In most cases, one image sized 800 × 600 can be segmented in 15 seconds using a personal computer (3.3GHz CPU, 4G RAM).

FIRST STAGE OF MATCHING

In this section we will introduce the first stage of the matching process of our proposed CMFD system. The three steps involved in this stage will be detailed in the following three subsections.

a. Keypoint Extraction and Description

In our implementation, we employ vlFeat3 [11] software to help us to detect and describe the keypoints. There are many kinds of keypoint detection and description methods. The common co-variant keypoint detection and description algorithms, such as difference of Gaussian (DoG), Harris-affine and Hessian-affine [8], [12], can provide similar detection performance. In our implementation we just employ the default setting of vlFeat for keypoints detection and description, namely SIFT [8]. Although the methods of keypoint detection and description are not rather important, note that the number of the keypoints should be larger than 2000 for good performance.

b. Matching Between Patches

Next we look for the suspicious pairs of patches that have many similar keypoints. This process is performed by comparing each patch with the rest. Define the distance between two keypoints by the L-2 norm of the difference between their descriptors. We should not take all the K searched keypoints into consideration, but only if the difference is smaller than a threshold then two keypoints are considered to be matched. Besides, like the traditional keypoint based CMFD schemes, we decrease the complexity of searching K nearest neighbors for a keypoint from O(n2) to O(nlogn), by constructing a k-d tree provided by vlFeat software[11].

c. Affine Transform Estimation

After detecting a suspicious pair of patches, we preliminarily know where the copying source region and pasting target region are. Then we estimate the relationship between these two regions in terms of a transform matrix H, such that

$$\overrightarrow{x'}=\mathrm{H}\,\overrightarrow{x}$$

where $\overrightarrow{x'}$and $\overrightarrow{x}$ are the coordinates4 of the pixels in the copying source region and pasting target region, respectively. Some proposed CMFD algorithms, especially the block-based ones [2]-[4] , only focus on finding the tampering regions and do not further investigate the transform relationship between the copying source region and pasting target region. In fact, it is rather helpful for the CMFD scheme to estimate the transform matrix between the two regions. Firstly, we are able to remove some falsely detected CMF regions as they do not have a set of points with uniform transform relationship. Secondly, more important, the CMFD is enhanced by providing the tampering detail about one image. So most recent CMFD algorithms choose to calculate the transform matrix [5]-[7]. As the existence of noise in the keypoints detection, we also employ the robust estimation method, namely RANSAC [9], to find a transform matrix H that is the best among a certain number of trials.

III. RESULT

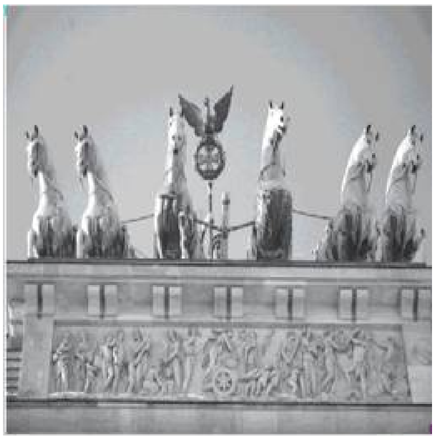

Fig 1: original picture

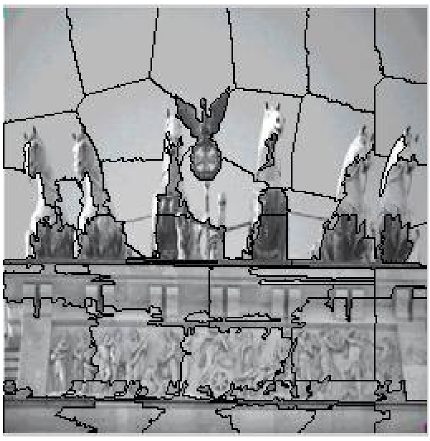

Fig 2: segmented picture

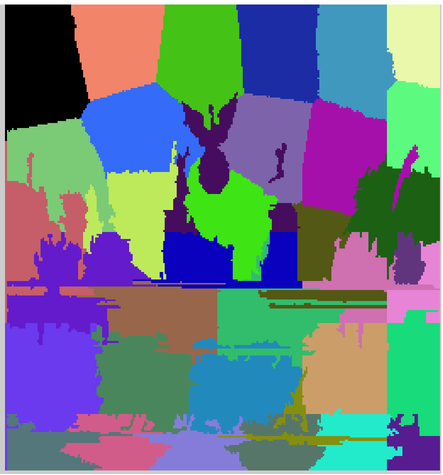

Fig 3: different patches with different Colour

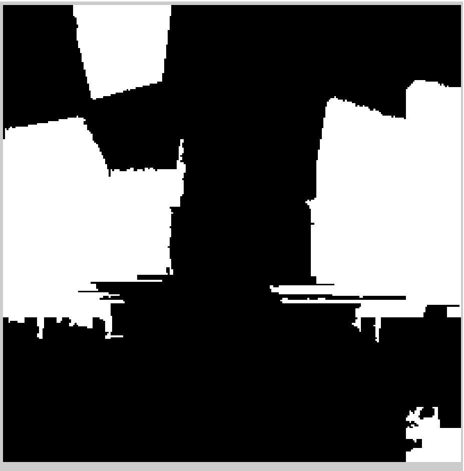

Fig 4: identification of copy move patch by keypoint extraction

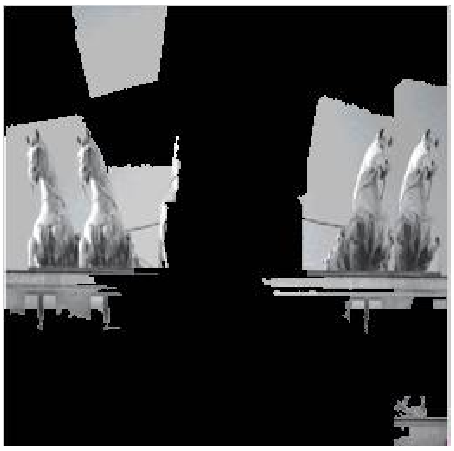

Fig 5: Final result , recovery of the image in the identified portion of copy move

IV. CONCLUSION

Region duplication is becoming an important issue and our paper describes an efficient method to solve this problem. Our method is based on SIFT features [8]which helps in matching the keypoint.For eliminating the unreliable keypoints RANSAC[9] algorithm performs well because correct matches need to have the closest neighbour significantly closer than the closest incorrect match to achieve reliable matching. For false matches, there will likely be a number of other false matches within similar distances due to the high dimensionality of the feature space. The result conclude that it is effective and robust in conditions like noise, and different JPEG qualities. Compared to other method where only matched key points are shown as detection results, we further estimate the transform between duplicated regions based on SIFT features[8] and recover the complete region contours using correlation map.

REFERENCES

[1] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[2] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, “Detection of copy-move forgery in digital images,” in Proc. Digit. Forensic Res. Workshop, 2003.

[3] W. Luo, J. Huang, and G. Qiu, “Robust detection of regionduplication forgery in digital image,” in Proc. 18th Int. Conf. Pattern Recognit. (ICPR), vol. 4. 2006, pp. 746–749.

[4] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Washington, DC, USA, Apr. 2009, pp. 1053–1056.

[5] V. Christlein, C. Riess, and E. Angelopoulou, “On rotation invariance in copy-move forgery detection,” in *Proc. IEEE Workshop Int. Inf. Forensics Secur. (WIFS)*, Dec. 2010, pp. 1–6.

[6] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[7] 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,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[8] D. G. Lowe, “Distinctive image features from scale-invariant keypoints,” *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, Nov. 2004.

[9] M. A. Fischler and R. C. Bolles, “Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography,” *Commun. ACM*, vol. 24, no. 6, pp. 381–395, Jun. 1981.

[10] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, “SLIC superpixels compared to state-of-the-art superpixel methods,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 11, pp. 2274–2282, Nov. 2012.

[11] A. Vedaldi and B. Fulkerson. (2008). *VLFeat: An Open and Portable Library of Computer Vision Algorithms*. [Online]. Available: http://www.vlfeat.org/

[12] K. Mikolajczyk *et al.*, “A comparison of affine region detectors,” *Int. J. Comput. Vis.*, vol. 65, nos. 1–2, pp. 43–72, Nov. 2005.