IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Based on Matching Process Recognition of Forger Image

Mr.Kolkure V.S.[1], Rekha H. Pawar[2]

Department of Electronics, Bharat Ratna Indira Gandhi College of Engineering, Solapur, India[1]

PG Student, Department Of Electronics, Bharat Ratna Indira Gandhi College of Engineering, Solapur, India[2]

Abstract: In today's environment seeing importance of digital data which is continuously increasing. The improvement in the digital data processing which leads to a low cost internet. With these improvement the copied image of forger can be detect. The copied image of forger can be detected by using segmentation and matching process. With these segmentation methods and matching process the copy move region can be detected. These two methods provide effective security and authentication to an image so that the misuse of images avoided. In this paper we detect the forger image.

Keywords: copied image, forger, segmentation, matching process, detection, etc.

I. INTRODUCTION

The experiment is carried out to with segmentation of test picture in to independent patches. This method helps in detection of copy move section [1].Image exploitation are very common now a days. The feature is to be added to reduce the illustration superiority of the image upon copying it. The SIFT classification is found useful to address this problem. Identifying the copied images is really very important [2]. Multimedia communication development leads to the development of security to the digital data. The privacy of the user is very important when using the systems online and offline. Stolen data is misused several times and may results in loss of money, time and privacy [3]. Image segmentation is required for identification of images. The modification in the images with bad intentions are noticeable is recent time. The images should not be copied without the permission of the original owner of the image. The digital evidences are considered legal in many criminal cases now days and hence the images are really important [4]. The digital data in any patterns should be preserved and protected. Many valuable information is shared and stored in digital form and hence its necessity of time to protect the data [5].

II. EXISTING SYSTEM

In this paper, we adopt a practitioner's view to copy-move forgery detection. If we need to build a system to perform CMFD independent of image attributes, which may be unknown, we create the realistic database of forgeries, accompanied by software that generates copy-move forgeries of varying complexity. We defined a set of what we believe are "common CMFD scenarios" and did exhaustive testing over their parameters. A competitive CMFD method should be able to cope with all these scenarios, as it is not known beforehand how the forger applies the forgery. We implemented 15 feature sets that have been proposed in the literature, and integrated them in a joint pipeline with different pre- and postprocessin g methods. Key point-based methods have a clear advantage in terms of computational complexity, while the most precise detection results can be achieved using Zernike moments.

III. PROPOSED METHOD

We propose a straightforward yet effective replacement for the shift vectors that can expressly handle affine transformations. The core idea is to explicitly estimate the rotation and scaling parameters from a few blocks, expressed as an affine transformation matrix. Starting from an initial estimate, we apply region growing on block pairs with similar transformation parameters. Consider the i-th matched pair ~fi of feature vectors ~fi1, ~fi2, ~fi = (~fi1, ~fi2). In order to determine the rotation and translation between block pairs, we need to examine the coordinates of the block centres. Let C(~fij) denote the coordinates (in row vector form) of the block center from where ~fij was extracted

$$\vec{p}_i = C(\vec{f}_{i1}), \qquad \vec{q}_i = C(\vec{f}_{i2}).$$

$$\vec{q}_i = \vec{p}_i \cdot A + \vec{b}$$

IV. METHODOLOGIES

Module 1: Image Segmentation
In this module first stage is extract the key points from the input image and produce a k-d tree. Then the KNN (k-nearest neighbour) search is used to work in each region for each key point to find a possible copied region. One region is recorded if it has a certain proportion of key points matched with another one. In this stage finally

estimate the affine relationship between the pairs of matches. The estimated transform matrix is given to the second stage of matching process, then refine the matrix via a probability model based on the EM algorithm. 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.

Fig A Segmented Image

Module 2: Key point Extraction And Description
This module is used to detect and describe the key points of extraction. There are various types of key points detection and description. The commonly used methods of key points detection and description are such as difference of Gaussian(DoG),Harris-affine and Hessian-affine .this The algorithm can provide similar detection performance .There are two methods which detect interest points in scale-space, and then determine an elliptical region for each point. The interest points are detected based on either harris detector or the Hessian matrix. In this two methods scale selection is based on the Laplacian. For feature detection or for local image structure autocorrelation matrix is used which is also called second moment matrix. The following are two gradient distributions:

$$M = \mu(\mathbf{x}, \sigma_I, \sigma_D) = \begin{bmatrix} \mu_{11} & \mu_{12} \\ \mu_{21} & \mu_{22} \end{bmatrix}$$

$$= \sigma_D^2\, g(\sigma_I) * \begin{bmatrix} I_x^2(\mathbf{x}, \sigma_D) & I_x I_y(\mathbf{x}, \sigma_D) \\ I_x I_y(\mathbf{x}, \sigma_D) & I_y^2(\mathbf{x}, \sigma_D) \end{bmatrix}$$

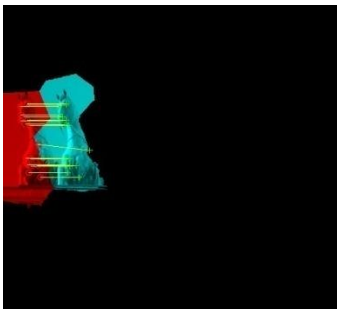

Fig B Example of patch matching

difference is smaller than a threshold (0.04 in our implementation), the two key points are considered to be matched. In other words, each key point in patch A is corresponding to no more than K key points in the remaining patches.

Module 4: Iterative Re-estimation of the transform matrix
In particular, the pixels not around the key points are abandoned. It is mainly because computer vision usually focuses on the research of transform estimation of two distinct images, in which case we are able to obtain a comparatively large number of matched key points. So in the second stage we propose to exploit all the pixels in the matched patches to find out a more accurate estimation H .Meanwhile, the pixels belonging to the CMF regions would be more clearly distinguished from the background
Since the really matched pixels in the copying source region and pasting target region should be close to each other, we change the definition of the relationship between them in Using the newly matched pixel pairs we wish to estimate a more convincing matrix H . Please note that some of these pixel pairs are outliers that are located outside the CMF region. Furthermore, some correspondences are not accurate enough because they may be at the smooth image regions. One natural solution is RANSAC as it is rather good at handling outliers .However, there usually are a large number of pixel pairs and hence RANSAC is too time-consuming.

This method enables the key points extraction and the local image derivatives are computed with Gaussian kernes of scale σD.

Module 3: Matching Between Patches
This methods perform the matching process between the patches. The patches have similar key points. The matching process is performed by comparing each patches with traditional method of patches. The distance between two key points by the L-2 norms .Let K is the nearest neighbours located in the patches. Let consider the example, there are more than one couple of copied region in the image ,let K=10. We should not take all the K searched key points into consideration but only if the

V. ADVANTAGES

1) Duplicated regions detect with changed contrast values and blurred regions can also be detected.
2) Robust and efficient method, detects post-processing effects like noise addition, blurring, lossy compression etc
3) Flat regions of forgeries are detected.
4) Efficient method, low false positives.
5) Can detect duplication even post-processing is done, robust and computationally less complex.
6) Can detect additive noise and lossy JPEG conversation.
7) Low computational complexity and robust to post-processing operations.
8) Working for post-processing like blurring, rotating, noise adding etc.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

9) Extracting features and sorting are done in different algorithms in parallel, less computational time, good for real-time applications.
10) False matches are reduced by considering matching of mutual pairs as well.
11) Efficient and robust to blurring, noise, scaling, lossy JPEG compression and translational effects.
12) Multi-dimensional and multidirectional gives precise results.

VI. APPLICATIONS

1) To controlled environments like military systems and surveillance cameras.
2) with infringement of copyright, blackmail, insurance fraud and other schemes based on digital forgery
3) Face recognition on out-of-focused photographs, template-to-scene matching of satellite images, in focus/defocus quantitative measurement, etc.

VII. HARDWARE REQUIREMENTS

Processor	: Pentium Dual Core 2.00GHZ
Hard Disk	: 40 GB
RAM	: 2GB (minimum)
Keyboard	: 110 keys enhanced

VIII. SOFTWARE REQUIREMENTS

MATLAB 7.14 Version R2012a

IX. RESULT DISCUSSION

In this proposed scheme we detect the forger image. So forger can not tampered the original image. If the forger shows the tampered natural images the shows the detection error in image level with false negative rate F_N and false positive rate F_P .The detection results of proposed scheme is based on SIFT and SURF.

X. CONCLUSION

This paper presented a CMFD scheme based on image segmentation. Although the CMF regions are detected mainly by comparing the key points extracted in the image, we can not simply classify the proposed scheme as a key point-based one .It can be seen as a combination of both existing schemes because in the two stages of matching process both key points and pixel features are employed. Our main contributions can be concluded to the following two aspects.

1. Considering the CMF regions usually have certain meaning, we propose to segment the image into semantically independent patches, such that the CMFD problem canbe solved by partial matching among these segmented patches.

2. The matching process between segmented patches consists of two stages. In the second stage, an accurate estimation of transform matrix can be obtained by an EM-based algorithm.

REFERENCES

[1] Li, Jian, et al. "Segmentation-based image copy-move forgery detection scheme." IEEE Transactions on Information Forensics and Security 10.3 (2015): 507-518..

[2] Amerini, Irene, et al. "Counter-forensics of SIFT-based copy-move detection by means of key point classification." EURASIP Journal on Image and Video Processing 2013.1 (2013): 1-17.

[3] Lian, Shiguo, Dimitris Kanellopoulos, and Giancarlo Ruffo. "Recent advances in multimedia information system security." Informatica 33.1 (2009).

[4] Chierchia, G., et al. "PRNU-based detection of small-size image forgeries." International Conference on Digital Signal Processing (DSP). 2011

[5] Lian, Shiguo, and Yan Zhang. "Multimedia forensics for detecting forgeries." Handbook of Information and Communication Security. Springer Berlin Heidelberg, 2010. 809-828.

[6] 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.

[7] P. Kakar and N. Sudha, "Exposing postprocessed copy–paste forgeries through transform-invariant features," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1018–1028, Jun. 2012.

[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] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "SURF: Speeded up robust features," Comput. Vis. Image Understand., vol. 110, no. 3, pp. 346–359, Jun. 2008.

[10] Q. Liu, N. Linge, and V. Lynch, "Implementation of automatic gas monitoring in a domestic energy management system," IEEE Trans. Consum. Electron., vol. 58, no. 3, pp. 781–786, Aug. 2012.

[11] Q. Liu, G. Cooper, N. Linge, H. Takruri, and R. Sowden, "DEHEMS: Creating a digital environment for large-scale energy management at homes," IEEE Trans. Consum. Electron., vol. 59, no. 1, pp. 62–69,Feb. 2013.

[12] M. A. Fischler and R. C. Bolles, "Random sample consensus: A para-digm for model fitting with applications to image analysis and automated cartography," Commun. ACM, vol. 24, no. 6, pp. 381–395, Jun. 1981.

[13] R. Hartley and A. Zisserman, "Multiple View Geometry in Computer Vision", 2nd ed. New York, NY, USA: Cambridge Univ. Press, 2004.

[14] M. Akhin and V. Itsykson, "Clone detection: Why, what and how?" in Proc. 6th Central Eastern Eur. Softw. Eng. Conf. (CEE-SECR), 2010, pp. 36–42.