ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

Image copy move forgery detection scheme

C.PRASANTH
ME (APPLIED ELECTRONICS)
TPGIT-VELLORE
prasanthmaxy97@gmail.com

PROF.S.KRITHIGA.M.E.
ASSISTANT PROPFESSOR
TPGIT-VELLORE

Abstract: A copy-move forgery is created by copying and pasting content within the same image, and potentially post processing it. This paper, propose a scheme to detect the copy-move forgery in an image, mainly by extracting the key points 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, find the suspicious pairs of patches that may contain copy-move forgery regions, and we roughly estimate an affine transform matrix. Refine the estimated matrix and to confirm the existence of copy move forgery.

***Index Terms*—Copy-move forgery detection, image forensics, segmentation**

I.INTRODUTION

An IMAGE with copy-move forgery (CMF) contains at least a couple of regions whose contents are identical. CMF may be performed by a forger aiming either to cover the truth or to enhance the visual effect of the image. Normal people might neglect this malicious operation when the forger deliberately hides the tampering trace (Figure 1). So we are in urgent need of an effective CMF detection (CMFD) method to automatically point out the clone regions in the image. And CMFD is become one of the most important and popular digital forensic techniques currently.

In the literature there are mainly two classes of CMFD algorithms. One is based on block-wise division, and the other on keypoint extraction. They both try to detect the CMF through describing the local patches of one image. The former first divides the image into overlapping blocks and then finds the CMF by looking for the similar blocks. Such a kind of method based on DCT describing the block, and they also decreased the complexity of the matching process by means of dictionary sorting. Because the descriptor of the block is important for the algorithm, various description methods like DWT, PCA etc were tested in these papers. Among them Zernike moment may be the best choice in terms of detection accuracy and robustness. Besides, some post-processing techniques were proposed to improve the CMFD algorithms' efficiency. The second class of algorithms detects the CMF through observing the key points in the image. SIFT and SURF might be the most widely used key points for CMFD .In some papper the authors estimated the transform matrix between the copying source region and pasting target region as well as detecting CMF in the image .In order to remove the effect of unwanted outliers, RANSAC was often employed to guarantee the robustness of the estimation. In the authors further improved the accuracy of the estimation result obtained by RANSAC via the gold standard algorithm. Because the number of the keypoints is much smaller than that of the blocks divided in an overlapping way, the keypoint-based algorithms require less computational resource than the block-based ones. Readers are referred to and for some survey and evaluation works.

Fig. 1. The left image gives the original image the images and right image gives the images with CMF.

In this paper we propose a new framework for CMFD. The test image is first segmented into non-overlapped patches. Then the mission of CMFD in one image is transfered to partial matching between the obtained patches, which is a problem having been deeply studied in the computer graph research domain. Based on the EM algorithm. We propose a new solution for the problem which has been proved to be an extension of the classic registration method iterative closest point (ICP). Our solution performs CMFD with two stages. The aim of the first stage is to find the suspicious matches, and a transform matrix between them is roughly estimated. Then in the second stage we confirm the existence of CMF by means of refining the transform matrix. Experimental results show that the proposed CMFD scheme outperforms most prior arts, especially the keypoint-based ones in terms of detection rate.

The rest of the paper is organized as follows. In Section II we first revisit the issues about CMFD and then show the framework of our proposed scheme based on image segmentation.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

Section III and IV describe the first stage and the second stage of matching process, respectively. The experimental results are given in Section V, followed by conclusion in Section VI.

II.OVERVIEW OF THE PROPOSED CMFD SYSTEM

In this section, via revisiting the important issues involved in CMFD we first give the framework of our proposed scheme, and then we explain the reason for using image segmentation.

A. The Framework of the Proposed Scheme

In order to obtain a convincing detection result we would always like to acquire as much forensic information as possible from the test image. So the mission of CMFD is not only to determine if an image has some regions containing identical contents, but also to locate these tampered regions. To this end, we can describe the image

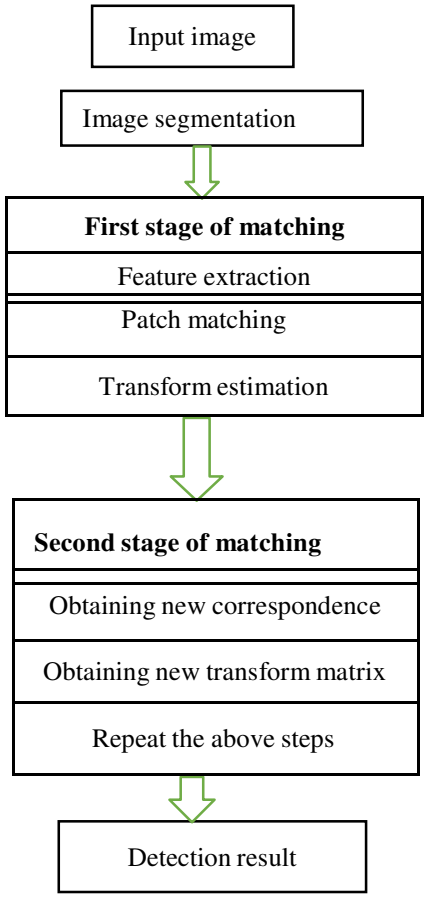

Fig.3.Block diagram proposed CMFD scheme

With a set of local patches, like the blocks or keypoints in traditional CMFD schemes, and transfer CMFD into a problem of comparison among these local patches. The comparison process may be time-consuming if the number of the patches is too large. For example, the block-based methods usually need a huge amount of time to detect an image. So it is important to decrease the number of patches for comparing. In this regard, the keypoint-based methods are faster and more favorable than the block-based ones, because the number of the image keypoints is smaller than that of the divided blocks.

However, on the other hand, keypoint-based method also has the following two problems. Firstly, the keypoints lying spatially close to each other should not be compared because they may be naturally similar.The determination of the shortest distance between two comparable keypoints is tricky. Most prior arts empirically select this threshold but neglect its relationship with the image size and content. Secondly, it is uneasy to accurately localize and distinguish the copying source region and the pasting target region, because, unlike the overlapping blocks, the keypoints are often not concentrated together. To deal with this problem 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. It is shown that the new clustering-based CMFD scheme significantly raise the accuracy of localization of CMF regions. We know that an image is seldom forged aimlessly. Hence the copy-move regions should have a certain meaning. In this light, we propose to segment the test image into a number of non-overlapped patches (refer to Figure 2). Then the CMFD can be performed by matching these patches, as long as the pasting target and copying source regions are not in the same patch.

B.*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. In our implementation however, we only consider the automatic approach and leave the expert interfering method for future work. After testing four famous image segmentation methods, it is observed that the segmentation method does not greatly influence the CMFD's efficiency. In most cases, one image sized 800 × 600 can be segmented in 15 seconds using a personal computer (3.3GHz CPU, 4G RAM). Figure 3 gives an example of image segmentation.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

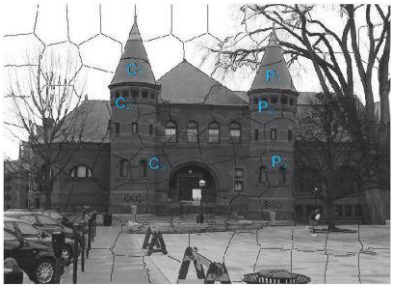

Fig. 3. Example of image segmentation

One may concern the scenario that segmentation cannot help us to separate the CMF regions into different patches. As mentioned above, in order that two CMF regions do not exist in the same patch, we should not coarsely segment the image. In our implementation, each image is empirically segmented into no less than 100 patches (refer to Section V for a further explanation), and thus, a CMF region may be in two or more patches (refer to Figure 3). In consequence the useful information for CMFD is reduced in each patch. However, to obtain a convincing detection result we need not a large number of keypoints (sometimes four is enough). Furthermore, because the CMF region exists in many patches, we meanwhile have more than one chance to find the tampering operation. Extensive experiments prove that the applied segmentation method is able to provide us with satisfying results.

III.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 (refer to Figure (2)) involved in this stage will be detailed in the following three subsections.

A. Keypoint Extraction and Description

In our implementation, we employ vlFeat[3] 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-affinecan provide sim- ilar detection performance. In our implementation we just employ the default setting of vlFeat for keypoints detection and description, namely SIFT. 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. Refer to Figure 4, assume that patch A is considered at this time. Define the distance between two keypoints by the L-2 norm of the difference between their descriptors. In patch A for each keypoint we search its K nearest neighbors that are located in the other patches. Considering there are usually more than one couple of copy-move regions in the image, we set $K = 10$ in our implementation. We should not take all the K searched keypoints into consideration, but only if the difference is smaller than a threshold (0.04 in our implementation), the two keypoints are considered to be matched. In other words, each keypoint in patch A is corresponding to no more than K keypoints in the remaining patches. We know that the target and source regions should have a large proportion of matched keypoints. If a large proportion of the matched correspondences of A are located in another certain patch, say B in Figure 4, A and B are considered to be a suspicious pair of patches where we may find CMF regions. So a threshold ϕ is defined to find the matched patches. In our implementation, ϕ is empirically set as 10 times the average number of keypoints per patch,

Fig. 4.Find the suspicious pair of patches

With the help of ϕ, most patches are eliminated from the estimation of transform matrix and, of course, the second stage of matching process. Besides, like the traditional keypoint- based CMFD schemes we decrease the complexity of searching K nearest neighbors for a keypoint from $O(n^2)$ to $O(nlogn)$, by constructing a k-d tree provided by vlFeat software

C. Affine Transform Estimation

After detecting a suspicious pair of patches, we preliminar- ily 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,

Some proposed CMFD algorithms, especially the block-based ones, 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 fo r the CMFD scheme to estimate the trans- form matrix between the two regions. Firstly, we are able to remove some falsely detected CMF regions as they do not have a

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

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 algrithms choose to calculate the transform matrix. In order to avoid leaving additional forgery traces in an image, the forgers often do not further change the copying source region. As a result, we can simply assume that the error of keypoints extraction only exists in the target regions.

And the estimation of transform between the source region and target region can be made by means of a classical method .That is, no less than three random non-collinear matched keypoints are first used to calculate the transform matrix H by means of minimizing the geometric distance . As the existence of noise in the keypoints detection, we also employ the robust estimation method, namely RANSAC to find a transform matrix H that is the best among a certain number of trials. This method is also adopted by some other CMFD schemes

IV.SECOND STAGE OF MATCHING

In the first stage of matching process, we have found the suspicious pairs of patches as well as the transform matrix between them. Although RANSAC can provide us with a robust estimation of transform matrix, it is still not accurate enough. Furthermore, some of these detected patches may be just false alarm containing not any CMF regions. In this section, we will introduce our second stage of matching process where the estimation of the transform matrix is refined via an EM-based algorithm. And the false alarm patches might also be eliminated in this stage

A. CMF Determination Based on Probability

In the first stage of matching process, we made use of the detected keypoints in the copying source region and pasting target region to estimate a transform matrix H.This process follows the traditional way of computer vision.In particular, the pixels not around the keypoints are aban- doned 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 larger number of matched keypoints. However, in the CMFD case the forgery regions are sometimes so small that only a limited number of keypoints can be detected there. As a result, the detection result of the first stage is not convincing because we do not have enough keypoints.

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

B.*Obtaining the New Correspondences of the Pixels*

Denote the transform matrix we estimated in the first stage by $H0$ for differentiation here. As $H0$ is not accurate enough, the x' obtained. May not be the real correspondence of x. So we search a new correspondence of x in the pasting target region, such that the pixel located at the new correspondence position is more similar to the pixel at $x\times$ than the old correspondence in terms of their local feature descriptions.

We first align the image by means of the estimated transform matrix, i.e. a new transformed image is obtained by,

$$\hat{I} = H^{-1} \cdot I.$$

C.Iterative Re-Estimation of the Transform Matrix

Using the newly matched pixel pairs we wish to estimate a more convincing matrix $\bar{H}$. 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 smooth 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.

We have two classes of pixels in each segmented patch. One is the CMF region, the other is the background. Distinguishing the CMF region from the background is the same problem as classifying these two kinds of pixels. We propose to employ the EM algorithm to this end. The EM algorithm is a useful method for statistical parameter estimation of the samples with underlying distributions. The algorithm repeats a procedure until a target variable converges. The procedure consists of an E-step and an M-step. In the E-step, we calculate the following value which is an expectation of the log likelihood $P(X, z| H_n)$, with respect to the conditional distribution $P(z| X, H_n-1)$, i.e.,

$$Q(H_n|H_n-1) = E_{z|X,H_n-1} \ln[P(X, z|H_n)],$$

V.EXPERIMENTAL RESULTS

A. Test Image Databases and Segmentation Settings

Two public available image databases involved in evaluation of our proposed CMFD scheme. The first one was constructed by Christlein , con- sisting of 48 base images and 87 copied

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

snippets that are pasted to the other locations in the same image to make the forgeries. These snippets are carefully selected .such that the CMF trace is almost unnoticeable. The original sizes of the images are rather large However, in some cases like the Internet and wireless multimedia applications, we are often faced with small sized images. So in our experiment the width and the height of the test images are set to no larger than 800 by means of resizing. Furthermore, we note that the process of resizing will make it difficult to extract keypoints from the CMF regions, which is rather challenging for the keypoint-based schemes

B.Error measures

The performance of the CMFD scheme is also tested by detection error at two different levels, namely image level and pixel level. The detection error at the image level is measured by the ratio of the missing detection to the forged images (i.e. false negative rate, FN), and the ratio of the false alarm to the original images

C. *Results on the First Database*

From this experimental result we can see the our proposed CMFD scheme is corresponding to the smallest false negative rate, which means the proposed scheme is good at detecting the tampered images. However, the false positive rate of the proposed scheme is also larger than the others. We think the reason is two-fold. First, the second stage of matching cannot remove all the false alarm from the output of the first stage of matching. On the other hand, when detecting the suspicious pair of patches its threshold ϕ is set as loose as possible to avoid miss of detection. In consequence, some images are falsely detected especially those with repeated contents, say Statue etc. Secondly, recall that we employ DSIFT to describe the pixels in the second stage of detection. DSIFT descriptor is fast and robust to attacks, but is not discriminative enough. These two problems need to be solved in our future work to essentially improve the efficiency of the proposed scheme. Figure 6 shows two tampered images that can only be detected by the proposed scheme.

As mentioned above our setting on the threshold ϕ is one important reason blowing the false positive rateup. Thus the false positive rate may be decreased simply by adjusting ϕ. We plot the ROC curve in Figure 7 to show the trade-off between false positive and false negative when changing ϕ.

It can be observed that the false positive rate can be smaller than 0.15 when set $\phi = 20$. However, the false negative rate is increased to 0.33 at the same time. So adjusting the parameter ϕ only allows us to satisfy different detection requirements, but it does not improve the performance of the proposed scheme essentially. Since the both test databases are not large enough, it is difficult to obtain a parameter setting suitable to every images based on the results. Thus we still set $\phi = 10$ in the following tests.

C.Test Results on MICC-F600

We also compare our proposed CMFD scheme with two prior arts on the database MICC-F600. It can be observed that the proposed scheme is with the lowest false negative rate but the highest false positive rate, which is rather consistent with the results on the benchmark database.The detection errors of the proposed scheme at pixel level for all the forged images are also calculated. The average *precision*, *recall* and $F1$ values are 0.86, 0.88 and 0.87, respectively. These results also prove the effectiveness of our segmentation setting.

VI.CONCLUSION AND DISCUSSION

This paper presented a CMFD scheme based on image segmentation. Although the CMF regions are detected mainly by comparing the keypoints extracted in the image, It can be seen as a combination of both existing schemes because in the two stages of matching process both keypoints and pixel features are employed. Our main contributions can be concluded to the following two aspects.

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

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

One may concern the computational complexity of the proposed scheme. Compared with the keypoint-based schemes, the proposed scheme mainly needs two more steps, namely the image segmentation and the transform estimation refinement. In our future work, we will try to improve the detection speed of the proposed scheme

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 region- duplication 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] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 1880–1883.

[6] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in *Proc. 18th Int. Conf. Syst., Signals Image Process. (IWSSIP)*, Jun. 2011, pp. 1–4.

[7] S. Khan and A. Kulkarni, "Detection of copy-move forgery using multiresolution characteristic of discrete wavelet transform," in *Proc. Int. Conf. Workshop Emerg. Trends Technol. (ICWET)*, New York, NY, USA, 2011, pp. 127–131.

[8] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1355–1370, Aug. 2013.

[9] 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.

[10] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA)*, vol. 2. Dec. 2008, pp. 272–276.

[11] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgery detection via texture description," in *Proc. 2nd ACM Workshop Multimedia Forensics, Secur. Intell.*, New York, NY, USA, 2010, pp. 59–64.

[12] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2010, pp. 889–892.

[13] X. Pan and S. Lyu, "Region duplication detection using image fea- ture matching," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[14] 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.

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

[16] D. G. Lowe, "Distinctive image features from scale-invariant keypoints,"

Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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