http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (14): 2975-2979, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.2975.2979

Exposing Copy-move Forgeries Based on a Dimension-reduced Sift Method

Haizhen He, Xinhang Huang and Jun Kuang
School of Information Science and Engineering Hunan University, Changsha, Hunan, 410082, China

Abstract: The idea of believing photographs to be true seems unreliable nowadays due to the availability of advanced image processing software. The proposed method investigates detecting copy-move forgeries. Firstly, the SIFT algorithm is applied to detecting keypoints in test images and keypoints are extracted as SIFT feature vectors. Secondly, in view of the complexity of computation, the PCA algorithm is used to reduce the dimension of SIFT feature vectors. Thirdly, a matching procedure is implemented in feature space of keypoints. Lastly, an agglomerative hierarchical clustering is performed on spatial location of matched keypoints to reduce the mismatched points. In the identification, conditions about the spatial distribution of keypoints are set to distinguish whether a test image is authentic. After the identification, the estimation of geometric transformation is carried out on tampered images through LMedS algorithm. Experiment and analysis show that the method is appropriate for the identification and estimation of copy-move forgery and can achieve a higher accuracy than existing methods with less dimension feature vectors.

Key words: Copy-move forgery, SIFT, PCA, LMedS, geometric transformation estimation

INTRODUCTION

A copy-move forgery denotes an image where part of its content has been copied and moved somewhere else with the intent to cover or emphasize an object within the same image (Fridrich *et al*., 2003). Simple forged images may only experience normal translation, but most forgeries may not contain a single translation. A lot of transformations, like scaling, rotation and so on, are applied to improve authenticity.

In order to detect these kinds of forgeries, many techniques were devised. The most common detecting methods are based on the blocked-based technique, which is to check small clusters or blocks of pixels for matches all across the image. This method, however, has two main drawbacks (Popescu and Farid, 2004). Firstly, the adaptability of this method is rather weak; secondly, making a successful detection consumes amount of computer resource. To avoid these problems, keypoint-based methods have been spurred on account of its robustness to many geometric transformations and relatively low computer resource demand. Amerini *et al*. (2011) achieved the detection of multiple copy-move forgery and the estimation of geometric transformations parameters successfully. But the estimation needs to set an empirical threshold and SIFT descriptor uses a rather complicated 128 elements vector to express the patch of pixels.

Our method avoids above problems through four aspects described below. Firstly, a dimension-reduced SIFT algorithm is utilized to extract feature vectors. Secondly, a dot product instead of Euclid distance is used for feature matching. Thirdly, considering the spatial distribution of keypoints in authentic images is different from that in tampered image, conditions about spatial distribution are set in our method. Lastly, the estimation of geometric transformation is achieved by LMedS algorithm.

The rest study is organized as follows. Section 2 briefly introduces the related works. Section 3 discusses the proposed approach in detail. Experimental results are reported in Section 4 and the conclusion is expressed in Section 5.

RELATED WORKS

The proposed method is based on the SIFT feature vectors extracted from keypoints and makes use of PCA to reduce the dimension of SIFT feature vectors after the extraction.

SIFT feature extraction: Through the analysis of local descriptors (Mikolajczyk and Schmid, 2005) and local affine region detectors (Mikolajczyk *et al*., 2005), SIFT features become a good choice for forgery detection because of their relatively strong robust performance and low computational resource demand.

Extracting a SIFT vector contains four major stages: (1) Scale-space extrema detection; (2) Keypoint localization; (3) Orientation assignment; (4) The

Corresponding Author: Haizhen He, School of Information Science and Engineering Hunan University, Changsha, Hunan, 410082, China

generation of keypoint descriptor. The SIFT descriptor has 128 elements, obtained from a 16×16 pixel area around the keypoint.

PCA: PCA makes use of dimension-reduced technique to transform variables into several main components (comprehensive variants) (Jolliffe, 1986). These main components can reflect the main information of original variables. They usually can be express as original variants linear combination.

PROPOSED METHOD

The eigenvectors extracted from forged regions will be similar to the ones extracted from tampered regions, because the original regions are basically the same as tampered regions. Therefore, comparing the dot products between the eigenvectors can be adopted for the task of detecting a forged part. The outline of our proposed method is shown in Fig. 1.

Extraction of SIFT features anddimension reduction: Once the test image is given, we can extract the feature vectors from keypoints. SupposeX = (x_1, x_2, ..., x_n) stands for the set of keypoints extracted from test image, their corresponding feature vectors are described as (f_1, f_2, ..., f_n) and every SIFT vector f_i contains 128 elements. The number of keypoints extracted from the image will be quite large and this will make matching procedure computationally impossible when the image resolution is high.

Therefore, in our method, the dimension of feature vectors is brought down by PCA algorithm after the extraction. During our experiments, the size of the dimension-reduced vector is reduced by nearly 75%. This improvement significantly lowers the pressure on computation resource and enhances the efficiency of features matching described below.

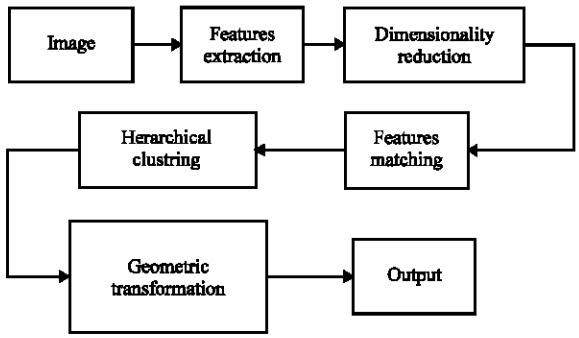

Fig. 1: Outline of proposed method

Features matching: To estimate the similarity between two vectors, first of all, the obtained feature descriptors (f_1, f_2, ..., f_n) are normalized to unit length. Note that the ratio of angles (arccosine of dot products of unit vectors) is a close approximation to the ratio of Euclidean distances for small angles and it's cheaper to compute dot products between unit vectors with respect to Euclidean distances. So, the second step is to compute the dot product between f_i and remaining (f_1,..., f_{i-1}, f_{i-1},... f_n). The third step is to calculate the arccosine of these dot products and sorting these values in ascending order (d_1, d_2, ..., d_{n-1}). As described by Amerini *et al.* (2011), we set the threshold T to 0.4 and iteratively compare d_i/d_{i+1} until the ratio is greater than preset threshold T. The first k items corresponding to (d_1, d_2, ..., d_k) may be matched points when this procedure stops at d_k, but the points which are too close will be abandoned.

Hierarchical clustering: Considering the fact that the keypoints of tampered areas tend to cluster in same regions of the image, while the mismatched ones will not follow this rule, checking the distribution of keypoints is important for detection. So we apply an agglomerative hierarchical clustering (Hastie *et al.*, 2005) on the spatial locations of keypoints to the identification of clone areas.

There is a need for the preprocessing of the matched points before clustering:

- **Step 1:** The matched keypoints between which the distance is below a certain threshold (like 45) will be abandoned
- **Step 2:** If the spatial distance between two points is quite close (lower than 10) as well as their matched points, these points will be abandoned
- **Step 3:** The points at the edge of an image will not involve our consideration

After the preprocessing has been accomplished, Single linkage method is listed below. Given two different clusters Γ_1 and Γ_2, x and y stand for the objects in the cluster Γ_1 and Γ_2.

Single linkage considers the smallest Euclidean distance between objects in two clusters:

$$\Delta_{single}(\Gamma_i, \Gamma_j) = \min_{\substack{x\in\Gamma_i \\ y\in\Gamma_j}} \delta(x, y) \quad (1)$$

According to the linkage method we adopted, we can get a specific tree structure. The next step is to cut this tree at an appropriate level by choosing a proper threshold. IC (inconsistency coefficient) characterizes the similarity between clusters, the higher this coefficient is

and the less similar these clusters will be, the clustering will stop when the coefficient is above the threshold. So a proper choice of the threshold will directly make an effect to our detection.

Geometric transformation estimation: LMedS (Rousseeuw and Leory, 1987) only focuses on the median of the distance between the original matched points and its corresponding estimated ones without cataloguing a point as inliers or outliers by a preset threshold.

Say that the matched points coordinates are $f_i = (x, y, 1)^T$ and $f_i' = (x', y', 1)^T$ for two different regions. We can use a 3×3 matrix H to define the geometric transformations between these two regions:

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \tag{2}$$

The matrix H, which is characterized as a perspective transformation matrix, has six variables waited to be computed:

$$H = \begin{bmatrix} a_{11} & a_{12} & | & a_{13} \\ a_{21} & a_{22} & | & a_{23} \\ 0 & 0 & | & 1 \end{bmatrix} \tag{3}$$

Let $(f_i', Hf_i)^2$ be the measurement of residual distance between the corresponding coordinates f_i', Hf_i:

$$(f_i', Hf_i)^2 = (x' - x_H)^2 + (y' - y_H)^2 \tag{4}$$

where, x_H, y_H stands for the coordinates which are calculated according to H.

All $(f_i', Hf_i)^2$ are sorted in descending order, suppose that R(i) stands for the rank of $(f_i', Hf_i)^2$, the ordering can be represented as:

$$(f_i', Hf_i)^2 \le (f_j', Hf_j)^2 \Leftrightarrow R(i) < R(j) \tag{5}$$

First of all, the LMedS algorithm estimates the transformation matrix H by randomly selecting three keypoints from a cluster and picking out their matched ones. The next step is to calculate the remaining keypoints' transformations according to H which we worked out at the first step. And the final step is to write down $(f_i', Hf_i)^2$ when m is the median of R(i). After iteratively execute above steps for N (N = 1000) times, the H leads to the lowest median $(f_i', Hf_i)^2$ is selected as the best model of the geometric transformation. So, the parameters of geometric transformation can be expressed as below:

$$\theta = \arctan\left(\frac{a_{21}}{a_{11}}\right), S_x = \frac{a_{21}}{\sin\theta}, S_y = \frac{a_{22}}{\cos\theta}$$

$$d_x = b_1, \; d_y = b_2$$

EXPERIMENTAL RESULTS

In this section, we present the results of our proposed methodology. In order to verify the availability of our proposed method, we tested it on database MICC-F220 (Amerini *et al*., 2011). This database contains 220 images, 110 are original images and 110 are tampered. The image resolution of this database ranges from 772*480 to 800*600 pixels and the forged part occupies 1.2% size of the image. These feigned images are obtained by copying and moving an image area to another region within the same image, furthermore some of the tampered regions are subjected to rotation and scaling transformations before pasting. Table 1 shows the geometric transformation parameters of these copy-move attacks, è° corresponds to rotation degree, S_x and S_y correspond to scaling factors applied to the x and y axis of the cloned image part, while the parameters of the translations are not shown because different images have different translations.

Forgery detection: After clustering was accomplished, we set conditions to determine the authenticity of a test image. These conditions can be divided into two aspects, one is about the number of points within a cluster and the other one is about the mutual distance of points within a cluster.

We start our work by checking the first part of conditions. The test image may be tampered if more than half of clusters contain more than 3 points, but we found this single condition may lead to a false alarm when one cluster contains most of points while the others contain a few points (Fig. 2). So, we add a condition that the largest cluster is more than two times larger than second largest one or more than four times greater than the third largest one (When the first three clusters contain different number of points). If one of these two conditions can be satisfied, this image meets the requirement of the number of points within a cluster in tampered image.

Table 1: Geometric transformation parameters applied to image patch

Attack	θ°	Sx	Sy
A	0	1	1
B	10	1	1
C	20	1	1
D	30	1	1
E	40	1	1
F	0	1.2	1.2
G	0	1.3	1.3
H	0	1.4	1.2
I	10	1.2	1.2
J	20	1.4	1.2

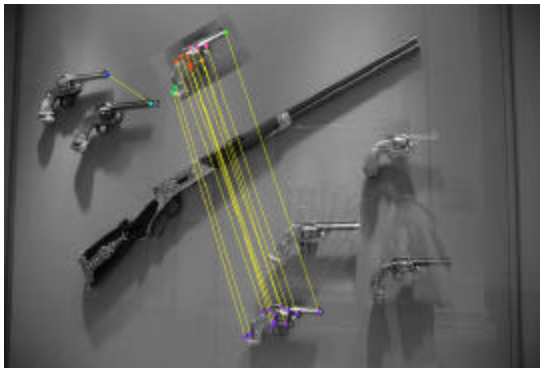

Fig. 2: Red points occupied most of keypoints while green one occupied a few ones

Fig. 3: Windows of the skyscraper are exactly the same

As for the second part of the conditions, the mutual distance of points within a cluster will be considered. In some scenario, authentic images also have matched keypoints because of similar objects in test image. As we can see in Fig 3, the windows of the skyscraper look exactly the same and their arrangement is highly intensive. In order to avoid this problem, we check whether a point and its matched point are clustered into same cluster (e.g.: in Fig. 3). If this sort of points does exist, we consider whether more than 60% points in one cluster belong to this type and the number of these points is greater than the quantity of matched pair in test image and more than half of these points and their matched ones have a mutual distance lower than 160. If the conditions above are satisfied while the points having a mutual distance less than 90 account for less than 50% whole points. The test image can be identified as an authentic image.

The performance of our method is measured in terms of TPR and FPR, TPR stands for the fraction of the correctly identified tampered images, while FPR is the fraction of incorrectly identified original images. The true positive rate TPR and false positive rate FPR for images are defined as follows:

$$TPR = \frac{\text{No. of forged images detected as forged}}{\text{No. of forged images}}$$

$$TPR = \frac{\text{No. of origional images detected as forged}}{\text{No. of origional images}}$$

Table 2: Detection results: FPR and TPR for *Single* linkage with respect to T_h

Th	FPR (%)	TPR (%)
0.8	7.34	68.18
1.0	5.50	75.45
1.2	5.45	96.36
1.4	4.55	97.27
1.6	0.91	100
1.8	0	100
2.0	0	100
2.2	0	99.09
2.4	0	98.18
2.6	0	98.18
2.8	0	98.18
3.0	0	97.27

Table 3: FPR, TPR and average processing time (per image) for each method

Method	FPR(%)	TPR (%)	Time (sec)
Fridrich *et al.*(2003)	84	89	294.69
Popescu and Farid (2004)	86	87	70.97
Amerini *et al.* (2011)	8	100	4.94
Our method	0	100	7.90

Table 4: Transformation parameters estimation errors

	MAE (θ)	MAE (Sx)	MAE (Sy)
A	0.172	0.011	0.003
B	0.501	0.016	0.028
C	0.485	0.013	0.022
D	0.423	0.015	0.021
E	0.591	0.016	0.021
F	0.279	0.016	0.005
G	0.237	0.011	0.013
H	0.620	0.020	0.007
I	0.292	0.017	0.009
J	0.239	0.022	0.022

In Table 2, we evaluate the effect of Single linkage with respect to different T_h. and the threshold T_h varies from 0.8 to 3.0 with the step of 0.2. The marked figures in Table 2 stand for the optimal parameters for forgery detection and the threshold T_h of Single linkage method leading to the maximum TPR is 1.8 and 2.0.

The final test results are reported in Table 3, we found Single linkage method works well. The crucial parameter which determines the final results of forgery detection is the threshold T_h.

Table 4 shows the performance and processing time for each method, the marked figures stand for the best results for each item. The detection performance of first

Table 5: MAE (θ), MAE (S_x) and MAE (S_y) for each method

	MAE (θ)	MAE (S_x)	MAE (S_y)
Amerini *et al.* (2011)	0.940	0.021	0.015
Our method	0.458	0.015	0.015

three methods is based on the information described by Amerini's work (Amerini *et al*., 2011). We can see that our method performs better than others in forgery detection. Although DCT and PCA methods obtain high TPR, they are unable to identify the authentic image. The time that our method consumes isn't the least, but we think the gap between our method and Amerini's (Amerini *et al*., 2011) is acceptable in view of the difference of computer configuration.

Our method works the best among these four methods especially for the identification of the authentic image. This significant improvement can be attributed to PCA algorithm and the extra conditions we set. The PCA algorithm brings down the mismatched feature vectors and extra conditions focus on the characteristic of the keypoints' distribution in authentic images. The progress on these two aspects makes our method more sensitive to authentic images.

Transformation parameter estimation: Table 5 reports the performance of proposed method on the estimation of geometric transformation. This table is composed of the absolute errors (|e|) between the original and estimated transformation parameters. MAE (θ) stands for the absolute errors between the original and estimated rotation angle, MAE (S_x) for the scale factor along the X-axis, MAE (S_y) for the scale factor along the Y-axis.

After checking all the tampered images in MICC-F220, we found that the estimated parameters are closed to their corresponding original ones. Table 5 shows the performance of the estimation of geometric transformations, the marked figures stand for the best results for each item. It can be seen that our method works better in the estimation of geometric transformation and this better performance relies on the high accuracy of previous identification.

CONCLUSION

In this study, we introduce a novel method for forgery detection. It is mainly based on a dimension-reduced SIFT algorithm and LMedS algorithm. The performance and efficiency of our proposed method has been showed in experiments and we established a method based on LMedS to achieve the estimation of geometric transformation. For further investigation, multiple copy attacks will be considered.

REFERENCES

Amerini, I., L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, 2011. A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inform. Forensics Security, 6: 1099-1110.

Fridrich, J., D. Soukal and J. Lukas, 2003. Detection of copy-move forgery in digital images. Proceedings of the 3rd Annual Digital Forensic Research Workshop, August 6-8, 2003, Cleveland, USA., pp: 174-184.

Hastie, T., R. Tibshirani, J. Friedman and J. Franklin, 2005. The elements of statistical learning: Data mining, inference and prediction. Math. Intelligencer, 27: 83-85.

Jolliffe, I.T., 1986. Principal Component Analysis. Springer-Verlag, Berlin, USA.

Mikolajczyk, K., T. Tuytelaars, C. Schmid, A. Zisserman and J. Matas et al., 2005. A comparison of affine region detectors. Int. J. Comput. Vision, 65: 43-72.

Mikolajczyk, K.I. and C. Schmid, 2005. A performance evaluation of local descriptors. IEEE Trans. Pattern Anal. Mach. Intell., 27: 1615-1630.

Popescu, A.C. and H. Farid, 2004. Exposing digital forgeries by detecting duplicated image regions. Department of Computer Science, Dartmouth College, Technical Report TR2004-515. http:// www.cs.dartmouth.edu/ reports/TR2004-515.pdf

Rousseeuw, P.J. and A.M. Leory, 1987. Robust Regression and Outlier Detection. 1st Edn., Wiley, New York, USA., ISBN-10: 0471852333, Pages: 352.