Copy-Move Forgery Detection using SIFT and GLCM-based Texture Analysis

Mohita Chowdhury, Hansal Shah, Theekshna Kotian, N Subbalakshmi and Sumam David S
Department of Electronics & Communication Engineering
National Institute of Technology Karnataka, Surathkal
Mangalore, India
chowdhury.mohita@gmail.com

***Abstract*—Easier access to editing tools and growing risk of image manipulation has encouraged extensive research in copy-move forgery detection. Although the current methods have been able to detect this tampering to a good extent, their accuracies drop when tested on images with different sizes of tampered regions and in the presence of similar but genuine objects in the image. In this paper, these issues are addressed by including a novel GLCM-based Texture Analysis Filter that gives information about the textural similarity of the keypoint neighbourhoods by using difference of GLCM contrasts as the similarity metric. Experimental results show that the proposed technique can address a variety of different tampering scenarios and outperforms the existing state-of-the-art Copy-Move Forgery Detection(CMFD) techniques by handling multiple forgeries, returning corresponding geometrical parameters and significantly improving the false positive rates.**

***Index Terms*—Gray-Level Co-occurrence Matrix, SIFT, Copy-Move Forgery Detection, Image Forensics**

I. Introduction

With better access to various image editing tools, the credibility of digital images is at stake. Images are used as a proof of reality - both in formal and informal settings and hence, its authenticity is of prime concern. In the past few years, the detection of tampered images has gathered much attention from researchers worldwide. A particular focus is given to copy-move forgery detection as it is one of the most commonly used image tampering techniques. Although there are methods dealing with this issue, they are not robust enough to handle realistic tampering or tampering where copied areas are subjected to different geometrical transformations. This calls for a need to have a technique that is not only immune to these processing steps but also differentiates well between actually copy-moved objects and Similar but Genuine Objects (SGO).

The Copy-Move Forgery Detection (CMFD) techniques available today can be mainly classified into block-based and keypoint-based techniques. In most real life scenarios, the copied region of an image is generally subjected to certain geometrical transformations, viz., scaling, rotation, etc., to evade detection. Although block-based techniques yield reasonably good results, these methods fail under the above stated conditions. On the other hand, keypoint-based techniques, apart from solving this problem, can be used to estimate the corresponding parameters of the geometrical transformations [1]. They are also robust to noise and JPEG compression [2]. In this approach, distinctive local features such as corners, blobs etc., are extracted and for each of these features, a descriptor is computed that describes their local neighbourhood. Today, although there are various keypoint detection methods like Speeded Up Robust Features (SURF) [3], Oriented FAST and rotated BRIEF (ORB) [4], Scale Invariant Feature Transform (SIFT) gives the most robust performance [5] [6].

In the past, copy-move forgery detection has been tried using various SIFT-based methods. Huang *et al.* [2] used SIFT to detect single copy-move forgery in images, making the algorithm robust to post processing operations like rotation, noise, JPEG compression, etc. In the approach presented in [7], rather than matching points, the proposed method matched clusters of points using SIFT which helped eliminate false positives. Amerini *et al.* [1] introduced generalized 2-Nearest Neighbour test (g2NN) for matching multiple forgeries undergoing various geometrical transformations and used hierarchical agglomerative clustering followed by Random Sample Consensus (RANSAC) for estimation of the parameters of the transformation. Discrete Wavelet Transform (DWT) was used to reduce the dimensionality along with SIFT in [8], and Stationary Wavelet Transform (SWT) was used in combination with SIFT in [9] to detect forgeries. Dense field technique that shows good accuracy but takes high processing time is used to detect tampering in [10]. In [11], the technique works based on the analysis of Delaunay triangles of local keypoints found using SIFT, SURF etc. Recently, Roy *et al.* [12] delved into the challenging but rarely attended problem of Similar but Genuine Objects (SGO) in Copy-Move Forgery Detection. They used Speeded-Up Robust Features (SURF) along with Rotated Local Binary Pattern (RLBP) features to make distinction between actually tampered and similar but genuine objects.

Although there are techniques existing in this domain, they perform well only with specific kind of images, for example when the tampered region occupies 1.2% of the whole image [1] etc. Some other methods are constrained only to correctly classifying similar but genuine objects in the image [12].

In this paper, a novel SIFT-based technique is proposed that uses gray-level co-occurrence matrix to refine the detected matches, so as to reduce false matching. The gray-level co-

978-1-7281-1895-6/19/$31.00 ©2019 IEEE

occurrence matrix found for the SIFT keypoint neighbourhood is used to find local contrast of the actual and forged areas, whose difference is used as a measure of similarity. The proposed technique significantly reduces false positive rates and removes false matches in tampered images, thus isolating the tampered region more accurately.

The rest of the paper is organized as follows: Section II introduces the proposed approach and presents theory on the concepts involved. Section III shows comparative results and conclusions are drawn in Section IV.

II. Proposed Approach

A. SIFT Keypoint Generation

Scale Invariant Feature Transform (SIFT) is a feature extraction algorithm which is invariant to scale, rotation and illumination. It is also immune to change in viewpoint. The algorithm is used to find keypoints in the image with the aforementioned properties. These properties make the detection in further stages immune to geometrical transformation. The keypoints are found in scale-space using difference of gaussian images. The detected scale-space extrema are further refined by using Taylor-series expansion up to quadratic terms and gradients as described in [5].

B. Keypoint Matching and Clustering

The keypoints and their 128-length descriptors obtained from SIFT algorithm are matched using generalised 2NN test as mentioned in [1]. This technique enables matching of multiple occurrences of the same features. In this technique, for each keypoint, a similarity vector D=$\{d_1, d_2, ...d_n\}$ is defined that represents its sorted euclidean distances with respect to the other descriptors in SIFT space. The ratio d_i/d_{i+1} is computed until the ratio exceeds a predetermined threshold (0.5 for the proposed method). If k is the index at which the procedure stops, each keypoint in correspondence to a distance in $\{d_1, d_2, ..., d_k\}$(where $1 \leq k \leq n$) is considered as a match for the inspected keypoint. These matched keypoints are then clustered using Agglomerative Hierarchical Clustering which is a bottom up approach used to find possible copy-moved patches in the image. Originally, each keypoint is assigned to a cluster, which is followed by merging the clusters based on reciprocal spatial distances between the clusters. This bottom up approach is continued until a final merging situation is obtained based on the linkage method used (ward's linkage for the proposed method) [1]. If there are at least two clusters matched by at least three points, the image is possibly forged [1] and is processed further. Otherwise it is classified as not tampered.

C. Refinement of Cluster Points using RANSAC

If the image satisfies the aforementioned cluster condition, RANSAC or Random Sample Consensus [13] is used to remove outliers in each cluster so as to compute accurate homography matrices for matched points. In this technique, random set of points (3 points for the proposed method) are taken to compute homography. This transformation is then applied back on other points in the cluster and the projected points are compared in terms of distance to the corresponding matched ones. Points having distance more than a certain threshold (0.05 for the proposed method) are classified as outliers. This process is repeated for a set number of iterations (3000 for the proposed method) and the transformation with the highest number of inliers is chosen. This homography matrix can be used to calculate rotation, translation and scaling as given in [1].

D. GLCM Contrast-based Texture Analysis of Centroid Neighbourhood

Gray-Level Co-occurrence Matrix or GLCM is used to analyse the textural properties of the image. The novel contribution of this paper is the usage of this technique to further refine matching regions and better understand if the region has been tampered or not.

RANSAC algorithm returns a set of inliers for the probable actual and matched points. In the proposed approach, the centroids for each actual and matched inliers set are computed and a 16×16 neighbourhood is considered around them. GLCM technique is applied on both the neighbourhoods and the contrast is calculated over these matrices. The contrast of GLCM gives information about the textural variation of the neighbourhood. Contrast is sometimes referred to as variance or inertia. It is calculated as follows:

$$Contrast = \sum_i \sum_j (i-j)^2 * p(i,j)$$

where $p(i,j)$ is the value of the normalised GLCM matrix at i^{th} row and j^{th} column.

The difference between the contrasts is an intuitive measure of the similarity between the neighbourhood. If the matched regions were indeed the part of the image, lighting, image contrast and other effects that occur because of natural photography and pose, might be different for the two. This will cause a slight difference in the contrast between the two similar but genuine regions. Hence we look at the contrast difference between the two regions (original and matching region that is probably tampered with). Here, we assume that the tampered region has been subjected to only geometrical transformations and compression and no linear or non-linear pixel intensity transformation.

After getting the RANSAC inliers, the centroids for two matching clusters are calculated. These centroids are used to make a 16×16 neighbourhood around them. The difference between the contrast values for the actual and matched neighbourhoods are then computed. A set of inliers is counted as tampered only if the contrast difference is less than the threshold T_c = 0.05. The threshold of 0.05 is empirically determined by running the approach over images from COVERAGE dataset as seen in Table IV. This threshold works well for other datasets as well. The proposed approach removes many random matches and hence refines the results as presented in the next section The approach is further illustrated in the flowchart given in Fig. 1.

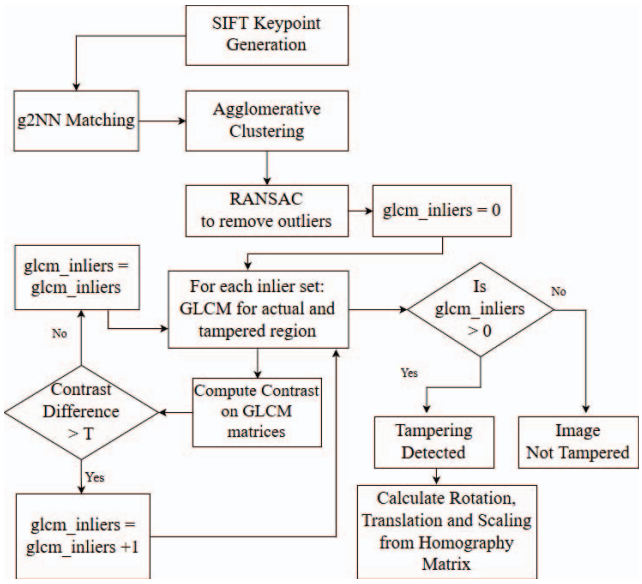
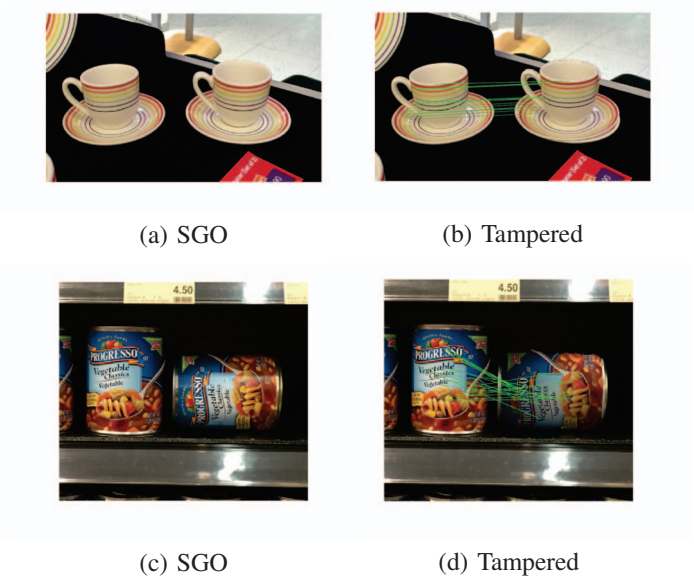


Fig. 1. Proposed Approach



(a) SGO (b) Tampered

(c) SGO (d) Tampered

Fig. 2. Results for Coverage dataset

III. Results

The proposed approach was tested on two single forgery datasets MICC-F220 [1] and COVERAGE [14] and on one multiple forgery dataset MICC-F8multi [1]. COVERAGE dataset consists of 200 images (100 original-forged image pairs) with average image size of 400×486 pixels and MICC-F220 has 220 images (110 tampered and 110 originals) with image resolution varying from 722×480 to 800×600 pixels, whereas MICC-F8multi has 8 images of 2048×1536 pixels, all tampered with one or more image regions copied and pasted in different positions multiple times. To the best of our knowledge, this is the first time when an approach has worked equally well on both COVERAGE (representative of SGO) and MICC (forged regions containing multiple geometrical transformations) datasets.

A. Qualitative Results

In the Fig. 2, a few results of the proposed method on the COVERAGE dataset are shown. The images (a) and (c) are genuine non-forged images, with very similar looking objects; they are correctly classified as non-tampered with zero final matches. Images (b) and (d) have undergone copy-move forgery and are correctly classified as tampered with good number of accurate matches. It can also very clearly be seen from image (d), that the algorithm works well even for large angles of rotation. Results from MICC-F220 and MICC-F2000 Dataset are presented in Fig. 3. The images are subjected to copy-move forgery under multiple geometrical transformations. The proposed approach identifies tampering and gives zero false matches in the images.

MICC-F8multi is a Multiple Forgery Dataset. Fig. 4 shows results from this dataset. The images are subjected to multiple copy-move forgery and the proposed approach is able to identify every forged region.

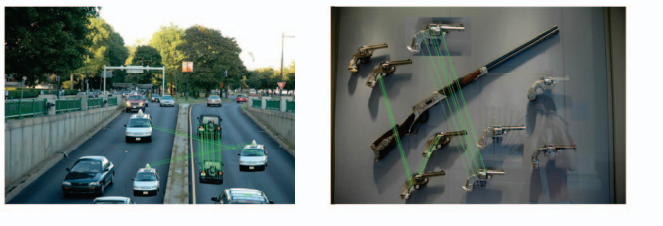
(a) MICC-F220(Tampered) (b) MICC-F2000(Tampered)

Fig. 3. Results for MICC single forgery dataset

B. Quantitative Results

The quantitative metrics are compiled below and are compared with the SIFT based [1] and RLBP-based [12] methods. Accuracy, False Positive Rate (FPR), True Positive Rate (TPR) and F-Score are calculated [1] [15] .

The geometrical parameters associated with the copy-move areas have been enlisted in Table I. To illustrate, one can observe that the matrix for rotation and scaling for the first



(a) MICC-F8multi(Tampered) (b) MICC-F8multi(Tampered)

Fig. 4. Results for MICC multiple forgery dataset

(a) Translation (b) Rotation and Translation

Fig. 5. Images with Geometrical Transformations

image 5(a), is a scaled identity matrix, which suggests that only translation took place for the given forgery. As seen from the image, the forged area is only translated and placed at the other location. Similarly for the second image 5(b), the matrix for rotation and scaling is the negative of an identity matrix, suggesting a 180° flip, which is indeed the geometrical transformation done on the image. The translation obtained from the homography matrix is the difference between the centroids of the actual and matched points.

As seen from the results in Table II, the SIFT-based approach [1] gives good accuracy for MICC-F220 but fails to give similar results for SGO dataset COVERAGE. The RLBP [12] approach gives good results on the COVERAGE dataset while results for MICC-F220 are not available. The proposed approach gives better accuracy than [1] and comparable accuracy to [12] for COVERAGE. Apart from that, it gives good results for MICC-F220 too.

From Table III, one can observe that [1] gives an FPR of 56% on COVERAGE dataset. This means that it classifies a lot of images with SGO as tampered. The proposed approach gives a significantly lower FPR of 34.34% on COVERAGE and 4.54% MICC-F220 hence showing improvement in false positive rates in both datasets. The FPR for RLBP [12] is not available.

Table IV shows some numerical results used to determine the threshold for contrast difference (T_c). The value of 0.05 gives the best set of metrics among all the other thresholds. This threshold works best for other datasets as well and hence the same T_c is used for other datasets.

IV. Conclusion

Robustly detecting copy-move forgery under the presence of similar but genuine objects and multiple geometrical transformations is important to cater to most real-life tampering scenarios. In this paper, an approach to tackle this based on the use of neighbourhood textural information using Gray-Level Co-occurrence Matrix along with SIFT, Agglomerative Clustering and RANSAC is proposed. Experimental results on different datasets like COVERAGE, MICC-F220 and MICC-F8multi prove that this approach surpasses other state-of-the-art algorithms dealing with similar problems in terms of significantly reduced false positives and better localisation of tampered regions. The proposed approach accurately finds the geometrical parameters and works robustly in different types of images.

TABLE I
Geometrical Parameters

Image	Transformation Matrix	Translation Vector
Fig.5(a)	$\begin{bmatrix} 1.662 & -0.000 \\ -0.001 & 1.665 \end{bmatrix}$	$\begin{bmatrix} -77.512 \\ -520.780 \end{bmatrix}$
Fig.5(b)	$\begin{bmatrix} -1.047 & -0.011 \\ -0.003 & -1.025 \end{bmatrix}$	$\begin{bmatrix} -0.030 \\ 0.162 \end{bmatrix}$

TABLE II
Accuracy of the proposed approach (GLCM) as compared to other approaches

Dataset	Only SIFT [1]	RLBP [12]	GLCM
COVERAGE	60.5%	70.5 %	70.07%
MICC-F220	96 %	NA	82.72%

TABLE III
FPR of the proposed approach (GLCM) as compared to SIFT-based approach [1]

Dataset	Only SIFT [1]	GLCM
COVERAGE	56%	34.34%
MICC-F220	9.09%	4.54%

TABLE IV
Quantitative Metrics for Contrast Difference thresholds T_c on COVERAGE dataset

T_c	TPR	FPR	Accuracy	F-Score
0.2	81.82%	47%	67.4%	71.11%
0.1	78.57%	42.42%	68.07%	70.37%
0.05	**74.49%**	**34.34%**	**70.07%**	**70.87%**
0.03	68.37%	28.29%	70.04%	68.36%

REFERENCES

[1] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copymove attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[2] Hailing Huang, Weiqiang Guo, and Yu Zhang, "Detection of copy-move forgery in digital images using sift algorithm," in *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*. IEEE, 2008, vol. 2, pp. 272–276.

[3] Herbert Bay, Tinne Tuytelaars, and Luc Van Gool, "Surf: Speeded up robust features," in *European conference on computer vision*. Springer, 2006, pp. 404–417.

[4] Ethan Rublee, Vincent Rabaud, Kurt Konolige, and Gary Bradski, "Orb: An efficient alternative to sift or surf," in *Computer Vision (ICCV), 2011 IEEE international conference on*. IEEE, 2011, pp. 2564–2571.

[5] David G Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of computer vision*, vol. 60, no. 2, pp. 91–110, 2004.

[6] Shaharyar Ahmed Khan Tareen and Zahra Saleem, "A comparative analysis of sift, surf, kaze, akaze, orb, and brisk," in *Computing, Mathematics and Engineering Technologies (iCoMET), 2018 International Conference on*. IEEE, 2018, pp. 1–10.

[7] Edoardo Ardizzone, Alessandro Bruno, and Giuseppe Mazzola, "Detecting multiple copies in tampered images," in *2010 IEEE International Conference on Image Processing*. IEEE, 2010, pp. 2117–2120.

[8] Mohammad Farukh Hashmi, Aaditya R Hambarde, and Avinash G Keskar, "Copy move forgery detection using dwt and sift features," in *Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on*. IEEE, 2013, pp. 188–193.

[9] Taposh Das, Rizbanul Hasan, Md Rasel Azam, and Jia Uddin, "A robust method for detecting copy-move image forgery using stationary wavelet transform and scale invariant feature transform," in *2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2)*. IEEE, 2018, pp. 1–4.

[10] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva, "Efficient dense-field copy–move forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284–2297, 2015.

[11] Edoardo Ardizzone, Alessandro Bruno, and Giuseppe Mazzola, "Copy–move forgery detection by matching triangles of keypoints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2084–2094, 2015.

[12] Aniket Roy, Akhil Konda, and Rajat Subhra Chakraborty, "Copy move forgery detection with similar but genuine objects," in *Image Processing (ICIP), 2017 IEEE International Conference on*. IEEE, 2017, pp. 4083–4087.

[13] Martin A Fischler and Robert C Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Communications of the ACM*, vol. 24, no. 6, pp. 381–395, 1981.

[14] Bihan Wen, Ye Zhu, Ramanathan Subramanian, Tian-Tsong Ng, Xuanjing Shen, and Stefan Winkler, "Coverage a novel database for copy-move forgery detection," in *IEEE International Conference on Image processing (ICIP)*, 2016, pp. 161–165.

[15] László A Jeni, Jeffrey F Cohn, and Fernando De La Torre, "Facing imbalanced data–recommendations for the use of performance metrics," in *Affective Computing and Intelligent Interaction (ACII), 2013 Humaine Association Conference on*. IEEE, 2013, pp. 245–251.