COPY MOVE FORGERY DETECTION WITH SIMILAR BUT GENUINE OBJECTS

Aniket Roy *Akhil Konda* *Rajat Subhra Chakraborty*

Dept. of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India 721302

ABSTRACT

Copy-Move Forgery Detection (CMFD) is a well-studied image forensics problem. However, CMFD with *Similar but Genuine Objects* (SGO) has received relatively less attention. Recently, it has been found that current state-of-the-art CFMD techniques are mostly inadequate in satisfactorily solving this important problem variant. In this paper, we have addressed this issue by using *Rotated Local Binary Pattern* (RLBP) based rotation-invariant texture features, followed by *Generalized Two Nearest Neighbourhood* (g2NN) based feature matching, hierarchical clustering and geometric transformation estimation. Experimental results show that our technique outperforms the state-of-the-art CFMD techniques for forged images having similar but genuine objects, and matches the accuracy of state-of-the-art techniques for other copy-move forgery types. Our method is also robust with respect to filtering and compression based post-processing.

Index Terms— Copy-move forgery, similar but genuine objects, Rotated Local Binary Pattern.

1. INTRODUCTION

Copy-move image forgery is a common tampering method in digital images. In such cases, some parts of the original image is copied and after some manipulation (i.e., scaling, rotation, illumination change etc.), pasted back onto the same image to generate the forged image. The existing *Copy-Move Forgery Detection* (CMFD) techniques in the literature can be classified into two major categories: (a) block based, and (b) keypoint based matching techniques. Fridrich et al. [1] proposed the first block based CMFD algorithm using *Discrete Cosine Transform* (DCT) and lexicographic ordering. Muhammad et al. [2] used *Dyadic Wavelet Transform* (DyWT) for CMFD utilizing approximation and detail subband statistics. Dimensionality reduction based techniques have been proposed in the literature using *Principal Component Analysis* (PCA) [3], *Singular Value Decomposition* (SVD) [4], etc. Besides, several techniques robust to geometric transformations have also been proposed using *Fourier-Mellin Transform* (FMT) [5], *Zernike Moment* [6], *Multi-resolution Local Binary Pattern* [7], etc.

This work is supported by *Science and Engineering Research Board (SERB)*, Govt. of India under Research Grant No. SB/FTP/ETA-0191/2013.

(a) **(b)**

Fig. 1. Example of copy-move forgery with SGO: (a) original image containing SGO, (b) forged image.

On the other hand, the keypoint based techniques are much more effective and computationally efficient. Huang et al. [8] proposed CMFD algorithm using *Scale Invariant Feature Transform* (SIFT), using number of matched features as a measure of image forgery. Pan et al. [9] improved the technique using affine transformation estimation among the matched SIFT keypoints. Amerini et al. [10] further improvised the scheme using hierarchical clustering of the matched features, followed by homography based geometrical transformation estimation. Detection of forged image is done based on the number of geometrical transformations found. Christlein et al. [11] provides an excellent survey and evaluation of popular CMFD approaches, along with a new copy-move forgery detection dataset, viz., 'Manipulate'. Computationally efficient *Speeded-Up Robust Features* (SURF) have been used by Xu et al. [12]. Recently, several CMFD techniques have also been proposed using *Harris points* and *step sector statistics* [13], *DAISY* descriptor [14], patchmark based *Dense-Field Descriptor* [15], etc.

Existing block and keypoint based CMFD algorithms treat region similarity as a measure of copy-move forgery, ignoring the fact that the realistic scene might contain *Similar but Genuine Objects* (SGO) as shown in Fig. 1. As the source of the forgery resides in the forged image itself, the CMFD problem is considered to be simply solved using region similarity. However, the same fact can make it difficult to detect the forgery for images having SGO. Wen et al. [16] introduced a novel image database *COpy-moVe forgERy dAtabase with similar but Genuine objEcts* (COVERAGE), and showed that the performance of the state-of-the-art techniques degrade significantly when applied to images containing SGO in the COVERAGE database. Since the state-of-the-art techniques find similar regions in both the authentic image with SGO,

and also the forged image, they are prone to substantial performance degradation due to false negatives. This motivates us to work on this important variant of the CMFD problem. Zhu et al. [17] obtained partial success in solving the problem with *Scaled Harris Feature Descriptor* (SHFD). However, for complex tampering (i.e., illumination change, free form and combination of these), their method performs only slightly better than the state-of-the-art SIFT [10], SURF [12] and Dense-Field [15] based approaches.

In this paper, we have used *Rotated Local Binary Pattern* (RLBP) features together with SURF based keypoints for more accurate CMFD detection, with images having SGO. **To the best of our knowledge, this is the first attempt to use RLBP for copy-move forgery detection.** The main insight behind our using the RLBP features, which is a rotation invariant texture feature set, is the fact that object embedding while performing copy-move image tampering produces unnatural local artifacts at the boundaries of the forged objects, thus making the forged image more textured than the original image. This observation also holds for the case of similar but genuine objects we are dealing with. Moreover, RLBP is geometric transform invariant. This justifies the supremacy of RLBP features over other feature sets used in state-of-the-art techniques. This is experimentally validated in the results section.

The rest of the paper is organized as follows. The proposed methodology is discussed in Sec. 2, followed by the experimental results in Sec. 3. Finally, conclusions are drawn in Sec. 4.

2. PROPOSED METHOD

The proposed methodology can be described into four main steps as follows: (a) Keypoint detection, (b) RLBP feature extraction, (c) Feature matching, and finally, (d) Clustering and forgery detection.

2.1. Keypoint Detection

We detect SURF interest points as keypoints for our scheme. SURF is a popular keypoint detector as well as descriptor proposed by Bay et al. [18]. However, we are only using the SURF keypoint detectors to find the high entropy keypoints in the image with lesser computational complexity. The keypoints are found by using a 'Fast-Hessian Detector', i.e., based on an approximation of the Hessian matrix of an given image point as described in [18].

2.2. RLBP feature extraction

Next, we extract the *Rotated Local Binary Pattern* (RLBP) features in a neighbourhood of the found SURF keypoints. RLBP is a rotation-invariant extension of the well-known efficient texture feature *Local Binary pattern* (LBP) [19]. LBP is computed in a local circular region by taking the difference of the center pixel with respect to its neighbouring grayscale values as follows:

$$LBP_{R,P} = \sum_{k=0}^{P-1} s(g_k - g_c) \cdot 2^k \tag{1}$$

$$\text{where} \quad s(g_k - g_c) = \begin{cases} 1, & \text{for } g_k \geq g_c \\ 0, & \text{for } g_k \leq g_c \end{cases} \tag{2}$$

Here, g_c and g_k denote the grayscale intensity values of the center pixel and its neighbours respectively, k denotes the index of the neighbour, R is the radius of the circular neighbourhood, P denotes the number of neighbouring pixels, and $s(g_k - g_c)$ denotes the weights of g_k with respect to the center pixel. LBP is not rotation-invariant. To overcome this shortcoming, recently, an improved rotation-invariant texture descriptor, namely *Rotated Local Binary Pattern* (RLBP) using dominant direction [19] has been proposed. The *dominant direction* (D) in a neighbourhood is the index of the neighbour whose difference to the center pixel is maximum, i.e.,

$$D = \max_{k \in (0,1,\ldots,P-1)} |g_k - g_c| \tag{3}$$

Since, the dominant direction would be invariant to rotation, thus a circular shift of the weights with respect to the dominant direction results rotation invariant RLBP features defined as:

$$RLBP_{R,P} = \sum_{k=0}^{P-1} s(g_k - g_c) \cdot 2^{(k-D) \,(\mathrm{mod}\, P)} \tag{4}$$

For each SURF keypoints, we take an 21×21 neighbourhood and find the $RLBP_{4,8}$ features for each keypoint. We take RLBP histogram as features; hence, feature dimension is 256. The rationale behind taking RLBP features is the fact that the tampered image must have some edge abnormality based artifacts during the copy-move operation, as explained previously. Hence, the forged image becomes more textured than the original image due to the local artifacts at the boundary of the forgery. RLBP, being an efficient texture feature along with its rotational invariance, is thus able to effectively discriminate between the original and forged image.

2.2.1. Illumination Invariance of RLBP

It has been observed that the CMFD performance (for images containing SGO) of the state-of-the-art schemes [10, 12, 15] degrade significantly with respect to copy-move forgery with illumination change operation. However, we take advantage of the fact that LBP features are illumination invariant [19]. In particular, we found RLBP to be more resistant to illumination modification than traditional LBP as it is computed taking difference of the pixel intensities with respect to the dominant direction, i.e., rotation invariant. Experimental results in Sec. 3 verify our claim for CMFD.

2.3. Feature Matching

After RLBP feature extraction, we use *generalized two Nearest Neighbourhood* (g2NN) based feature matching technique [10] to find the matches between the feature space. Initially, the best candidate match for each keypoint is found by identifying its nearest neighbour from all other keypoints of the image, which is the keypoint with minimum Euclidean distance in the feature space. However, this has been improved by using 2NN test that considers the ratio between the distance of the candidate match and distance of the second nearest neighbour, and compares whether it is lower than a predefined threshold (T). For example, given a keypoint, suppose the vector $D = \{d_1, d_2, \ldots, d_n\}$ represents sorted Euclidean distances with respect to other descriptors. Then, the keypoint is matched if $d_1/d_2 \leq T$.

The g2NN further generalizes the matching considering iterative 2NN test between d_i/d_{i+1}, until the ratio becomes larger than a defined threshold (T). The corresponding matches for the keypoint will be the keypoints with distance in $\{d_1, d_2, \ldots, d_k\}$, where k is the value where the process stops. In our experiments, we take threshold, $T = 0.5$.

2.4. Clustering and Forgery Detection

Next, to identify the possible similar areas, an *Agglomerative Hierarchical Clustering* [20] scheme with *Ward's linkage* [10] is performed on the spatial location of the matched feature points. This clustering generates tree-structured hierarchy of clusters. Initially, each keypoint is assigned to a cluster, then all the reciprocal spatial distances among the clusters are computed and based on that the closest pair of clusters is found and finally merges them to a single cluster. The process is iterated repeatedly until the linkage based final merging happens.

Suppose two clusters A and B contains n_A, n_B objects respectively, and x_{Ai}, x_{Bj} denote the $i-th$ and $j-th$ object in the clusters respectively. Then, *Ward's linkage* evaluates the increment/decrement in the error sum of squares (ESS) after merging the two clusters into a single one with respect to the case of two separated clusters:

$$d_{dist}(A, B) = ESS(AB) - [ESS(A) + ESS(B)] \quad (5)$$

where, with $\overline{x_A}$ denoting the arithmetic mean of the cluster A, and,

$$ESS(A) = \sum_{i=1}^{n_A} |x_{Ai} - \overline{x_A}|^2 \quad (6)$$

The clustering procedure groups the keypoints that are spatially close. Finally, the clusters having less than three keypoints are eliminated. After clustering, we take three matched point pairs between each clusters to compute an affine transformation in order to estimate the geometrical transformation between matched points among the clusters.

Suppose, the coordinates of the matched points be $\{(\mathbf{x_1}, \mathbf{x'_1}), \ldots, (\mathbf{x_k}, \mathbf{x'_k})\}$, where keypoint coordinates are denoted as, $\mathbf{x_i} = (x_i, y_i)$. Here, keypoint $\mathbf{x}$ resides in one cluster and keypoint $\mathbf{x}'$ resides in another cluster. Then the affine transformation can be expressed as:

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \mathbf{H} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \quad (7)$$

where $a_{11}, a_{12}, a_{21}, a_{22}$ denote the rotation and scaling direction deformation; t_x, t_y denote the translational counterpart; $\mathbf{H}$ denotes the affine homography which is estimated by *normalized direct linear transform* (DLT) [21]. To eliminate false matches *RANdom SAmple Consensus* (RANSAC) is used [21]. For each cluster pair (corresponding to original and cloned region) an affine transformation is estimated [22]. If the count of the total estimated affine transformation is non-zero, then the corresponding image is considered to be forged. The primary idea is that forged image contains similar region which can be described by a geometric transform, which is not in the case of an original image.

3. EXPERIMENTAL RESULTS

3.1. Experimental Setup

We have evaluated our approach with the state-of-the-art SIFT [10], SURF [12], Dense-Field [15], SHFD [17] based methods, on the recently proposed COVERAGE dataset which contains 100 pairs of original and copy-move forged image containing SGO. Forged images undergo six different types of tampering, viz., translation, rotation, scaling, illumination, free-form and combined factors. We have also experimented our technique on other benchmark database, viz., *CoMoFoD* [23] and *Manipulate* [11]. To evaluate the performance of CMFD, we have used detection accuracy (Acc) as a metric:

$$Acc = \frac{TP + TN}{TP + TN + FN + FP} \times 100(\%) \quad (8)$$

where TP, TN, FP, FN denote true positive (correctly predicted tampered), true negative (correctly predicted authentic), false positive (authentic predicted as tampered) and false negative (tampered predicted as authentic).

3.2. Comparison with State-of-the-art

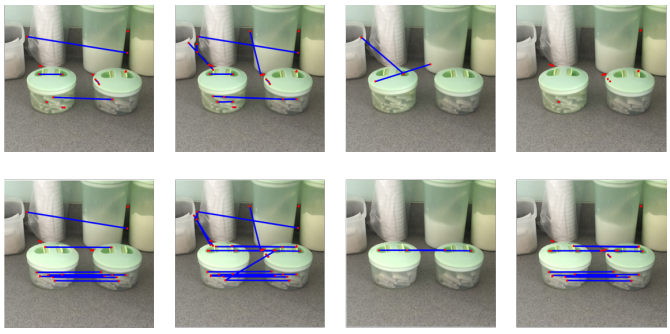
Comparison against several state-of-the-art techniques (with different attacks involved) in Table 1 exhibits that our proposed technique is the best in the case of COVERAGE dataset and also performs consistently well with respect to other datasets as shown in Table 2 when compared to the state-of-the-art. Fig. 2 and 3 also verify that visually. Table 1 also shows that our scheme performs better than the existing schemes with respect to illumination, free-form based

Table 1. CMFD detection accuracy (%) comparison for COVERAGE with the state-of-the-art

Operation (# test image)	SIFT [10]	SURF [12]	SHFD [17]	Dense Field [15]	Proposed scheme
Translation (16)	50.0	75.0	75.0	**93.8**	**93.8**
Scale (16)	56.3	56.3	50.0	**75.0**	50.0
Rotation (16)	46.7	53.3	56.2	**86.7**	62.5
Free-form (16)	43.8	50.0	45.0	68.8	**75.0**
Illumination (16)	43.3	62.5	45.0	62.5	**81.3**
Combined (20)	**55.0**	**55.0**	43.7	50.0	45.0
original (100)	71.8	52.3	64.6	60.2	**73.0**
Total (200)	60.5	55.5	58.5	66.5	**70.5**

Table 2. Detection Accuracy comparison for other databases

CMFD database (# test image)	SIFT	SURF	SHFD	Proposed Scheme
CoMoFoD (200)	**77.0**	51.5	27.0	70.1
Manipulate (48)	75.0	58.3	20.8	**83.3**



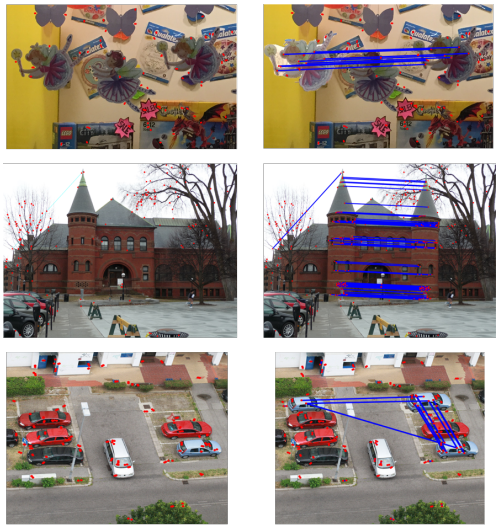
(a) SIFT (b) SURF (c) SHFD (d) RLBP

Fig. 2. CMFD performance comparison of SIFT [10], SURF [12], SHFD [17] and proposed RLBP based schemes (illumination tampering) on COVERAGE image database. The upper row contains original images with SGO, lower row contains forged image. Dots and lines denote keypoints and matched pairs respectively.

attacks on the COVERAGE dataset. For other attacks also our scheme performs comparably with the state-of-the-art. The best CMFD result is marked in bold. We have taken $RLBP_{4,8}$ in all our experiments with feature radius 4, as this gave best result with respect to CMFD accuracy as shown in Fig. 4.

3.3. Experiments on Post-processed Tampered Images

We have also verified the robustness of our technique with respect to different post-processing techniques applied on the tampered images, viz. compression, blurring, etc. We modified the images from the COVERAGE dataset using JPEG compression (with quality factors $Q \in \{60, 80\}$) and Gaussian blurring (window size $w = 3$ and sigma $\sigma \in \{0.5, 1\}$). Experimental results in Table 3 show that our scheme is robust to this post-processing with respect to the state-of-the-art methods on the COVERAGE dataset.



(a) Original (b) Forged

Fig. 3. Comparison of proposed scheme in different databases: COVERAGE (first row), Manipulate (second row) and CoMoFoD (third row).

Table 3. Det. Acc. after Post-processing for COVERAGE

Post processing operation	SIFT	SURF	Dense Field	SHFD	Proposed Approach
Compression (Q=80)	56	53.5	66.5	57.5	**70.5**
Compression (Q=60)	54	54	**66.5**	42	65.5
Blurring ($\sigma = 0.5$)	60.5	55	66	56.5	**68**
Blurring ($\sigma = 1$)	60	55.5	**65**	54	64.5

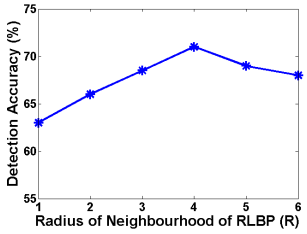


Fig. 4. Variation of CMFD accuracy with RLBP radius in COVERAGE dataset.

4. CONCLUSION

Copy-move forgery detection with SGO has been found to be more challenging than the existing CMFD techniques in the literature which depend mainly on region similarity based metrics for forgery detection. In this paper, RLBP features are used along with g2NN feature matching, hierarchical clustering, and geometric transformation estimation for efficient CMFD with SGO has been proposed. Our approach performs best for the COVERAGE dataset and also consistently for other databases for CMFD with respect to the state-of-the-art. The scheme is also robust to post-processing of the forgery.

5. REFERENCES

[1] A Jessica Fridrich, B David Soukal, and A Jan Lukáš. Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*. Citeseer, 2003.

[2] Ghulam Muhammad, Muhammad Hussain, and George Bebis. Passive copy move image forgery detection using undecimated dyadic wavelet transform. *Digital Investigation*, 9(1):49–57, 2012.

[3] Alin C. Popescu and Hany Farid. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[4] XiaoBing Kang and ShengMin Wei. Identifying tampered regions using singular value decomposition in digital image forensics. In *Computer Science and Software Engineering, 2008 International Conference on*, volume 3, pages 926–930. IEEE, 2008.

[5] Weihai Li and Nenghai Yu. Rotation robust detection of copy-move forgery. In *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pages 2113–2116. IEEE, 2010.

[6] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee. Detection of copy-rotate-move forgery using zernike moments. In *International Workshop on Information Hiding*, pages 51–65. Springer, 2010.

[7] Reza Davarzani, Khashayar Yaghmaie, Saeed Mozaffari, and Meysam Tapak. Copy-move forgery detection using multiresolution local binary patterns. *Forensic science international*, 231(1):61–72, 2013.

[8] 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*, volume 2, pages 272–276. IEEE, 2008.

[9] Xunyu Pan and Siwei Lyu. Region duplication detection using image feature matching. *IEEE Transactions on Information Forensics and Security*, 5(4):857–867, 2010.

[10] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. A sift-based forensic method for copy–move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security*, 6(3):1099–1110, 2011.

[11] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou. An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security*, 7(6):1841–1854, 2012.

[12] Xu Bo, Wang Junwen, Liu Guangjie, and Dai Yuewei. Image copy-move forgery detection based on surf. In *Multimedia information networking and security (MINES), 2010 international conference on*, pages 889–892. IEEE, 2010.

[13] Likai Chen, Wei Lu, Jiangqun Ni, Wei Sun, and Jiwu Huang. Region duplication detection based on harris corner points and step sector statistics. *Journal of Visual Communication and Image Representation*, 24(3):244–254, 2013.

[14] Jing-Ming Guo, Yun-Fu Liu, and Zong-Jhe Wu. Duplication forgery detection using improved daisy descriptor. *Expert Systems with Applications*, 40(2):707–714, 2013.

[15] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva. Efficient dense-field copy–move forgery detection. *IEEE Transactions on Information Forensics and Security*, 10(11):2284–2297, 2015.

[16] Bihan Wen, Ye Zhu, Ramanathan Subramanian, Tian-Tsong Ng, Xuanjing Shen, and Stefan Winkler. Coveragea novel database for copy-move forgery detection. In *Image Processing (ICIP), 2016 IEEE International Conference on*, pages 161–165. IEEE, 2016.

[17] Ye Zhu, Tian-Tsong Ng, Xuanjing Shen, and Bihan Wen. Revisiting copy-move forgery detection by considering realistic image with similar but genuine objects. *arXiv preprint arXiv:1601.07262*, 2016.

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

[19] Rakesh Mehta and Karen O Egiazarian. Rotated local binary pattern (rlbp)-rotation invariant texture descriptor. In *ICPRAM*, pages 497–502, 2013.

[20] Jerome Friedman, Trevor Hastie, and Robert Tibshirani. *The elements of statistical learning*, volume 1. Springer series in statistics Springer, Berlin, 2001.

[21] Richard Hartley and Andrew Zisserman. *Multiple view geometry in computer vision*. Cambridge university press, 2003.

[22] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, and Giuseppe Serra. Copy-move forgery detection and localization by means of robust clustering with j-linkage. *Signal Processing: Image Communication*, 28(6):659–669, 2013.

[23] Dijana Tralic, Ivan Zupancic, Sonja Grgic, and Mislay Grgic. Comofodnew database for copy-move forgery detection. In *ELMAR, 2013 55th international symposium*, pages 49–54. IEEE, 2013.