Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)
IEEE Xplore Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1

Efficient Keypoint based Copy Move Forgery Detection Method using Hybrid Feature Extraction

Sunitha K[1], Krishna A N[2],*Member,IEEE*
Department of CSE
SJB Institute of Technology, Bengaluru and affiliated to
Visvesvaraya Technological University, Belagavi, Karnataka, India
sunitha_k11@yahoo.com[1], ankrishna@sjbit.edu.in[2]

***Abstract*—Digital images are considered as one of most sorted mediums as an evidence or proof in various areas. For example, in forensic analysis, military intelligence, medical imaging, journalism, crime scene investigation and so on. With increased use of smart phones and cheap availability of internet has led to increased circulation of digital image. Along with, availability of wide range of digital image editing tools has made tampering image much easier. Such tampered image generates an improper message and could be used to influence events especially when the society based important decisions are carried out using these tampered image. Copy move tampering method has been widely applied passive image tampering method. Extensive work has been carried out in recent time for detecting such copy move tampering attack using key-point and block based method. However, these methods does not extract enough feature points considering small and smoothed region. For overcoming research challenges, this paper presents an efficient copy move forgery detection(CMFD) technique using key-points employing hybrid feature extraction, detection and hierarchical clustering method. Experiment result shows the proposed method attain significant performance when compared with other forgery detection methods.**

Keywords— Image forgery detection, feature extraction, key point extraction, clustering, CMFD.

I. INTRODUCTION

Currently even with the quick growth of technology, images and videos continue to be primary sources of information. They are the latest important information carriers in research fields such as forensic analysis, satellite image analysis, object tracking, remote sensing and photogrammetry [1], [2]. However, the widespread popularity of multimedia editing softwares such as Adobe Photoshop have increased the convenience of image editing. While multimedia that has been tampered with, can make people's lives more interesting, such tampering also poses a threat in many fields [3], particularly those that involve legal and safety aspects such as insurance claims, court sentences, patent infringement, medical diagnoses and so on. Image forgeries (IF) are of various sorts, for example, splicing [2], copy move forgery (CMF) and so on. CMF is one of the most well-known kind of tampering, where both the forged and pasted segments is within the image itself. Along these lines, both segments (i.e., original and forged segments) have comparable feature sets such as pattern, shading component, noise, color, contrast and so on. Thus, makes tampering detection a very challenging and difficult task. Recently, number of methods have been presented for addressing CMFD. These methods are either block or keypoint based CMFD method.

Block based strategies [4], [5], [6], [7] segments out the given input image into overlapping or non-overlapping block sets. Further, for each individual block set feature vector (FV) is extracted. Then, FV matching is carried out among FV's for establishing identical block sets. However, the block based technique generally induce high computation overhead. Then again, keypoint based tampering detection techniques [2], [4] are quicker for establishing feature sets. Along with, they are progressively robust against different operations and affine transformation (AT).

Keypoint based tampering detection strategy is composed of following steps such as keypoint sets detection, descriptions, and matching. For describing keypoint sets, different feature sets are utilized. In [8], proposed a CMFD scheme that used the Scale-Invariant Features Transform (SIFT) feature, which is insensitive to geometric transformation and illumination distortion. Further, [9] presented a J-linkage algorithm, which implements a robust cluster in the space of a geometry transformation to enhance the model of [8]. In [10], proposed a CMFD scheme based on Speeded Up Robust Features (SURF) [11] and used a k-dimensional tree (k-d tree) to search for similar SURF descriptors. However, the duplicated regions are indicated by lines and the boundaries of the duplicated region are not explicit. Keypoint based techniques are much quicker for establishing feature sets in any event, for enormous size pictures. This is because the keypoint based method establish and match FV using detected keypoint sets. SURF feature detector are much quicker. That is, they are 2 to 3 times much quicker than SIFT. This is due to usage of integral image and Box Filters (BF). After identifying identical keypoint descriptors, BF is used for

removing mismatches considering certain pre-established thresholding parameter.

Likewise, a discretionary post-processing operation can be carried out for grouping matches that resemble similar affine transformation pattern. In spite of the fact that keypoint based techniques are computationally much quicker, identifying tampering of small and smooth segments is a difficult task. The test fundamentally originates from the way that the quantity of keypoints are constructed or obtained on the smooth and small size object sets will be generally very less. Further, these model cannot be applied for detecting forgery where quantity and quality of feature point extracted play a significant factor. For overcoming research challenges this work present efficient key-point based CMFD (EKP-CMFD) method by combining SURF detector, SIFT descriptor, hierarchical clustering technique and RANSAC(Random Sample Consensus).

Research Contributions are as follows:

- Presents an efficient keypoint based copy move forgery detection method using hybrid feature extraction method (i.e., SURF is utilized as feature detection whereas SIFT is utilized as feature descriptor).
- Agglomerative hierarchical clustering method is used for feature matching. Further, the outliers are removed and image is transformed using RANSAC.
- Experiment outcome shows proposed model attain superior performance when compared with existing CMFD method in terms of evaluation metrics such as recall, FPR, and F1-score.

This paper organization is as follows: The proposed efficient key point based image tampering detection method is presented in section II. The experimental analysis is presented in the section III. In last section, the research work is concluded with future research direction.

II. AN EFFICIENT KEYPOINT BASED COPY MOVE FORGERY DETECTION METHOD

This work first present an efficient keypoint based CMFD method. The architecture of proposed efficient keypoint based CMFD is presented in Fig. 1. The methodology to overcome the above research problem is discussed below. First, the image will be segmented into equal patch or block size. Then SURF detector and SIFT descriptor are used for extracting keypoints. Then, agglomerative hierarchical clustering method is used for matching feature points. Lastly, for eliminating mismatches (i.e., outliers) and estimating image transformation RANSAC is used.

a) Dividing Image into equal patch size:

Preprocessing involves dividing image into equal size patches. As copy moved parts are from the same image, a correlation is established between them. This correlation forms a basis for successful detection of this type of forgery. Because of the possibility of retouching operation and saving in a lossy compressed format, the copy moved parts may not match exactly.

b) Keypoint detection using SURF and Descriptor using SIFT:

The SURF [13] technique is widely used and known feature detector that is scale invariant in nature. The SURF is designed using fast approximation of the Hessian matrix (HM) [13]. For reducing computation overhead, the SURF use integral image for approximating HM in adaptive manner. For approximating, SURF used set of BFs. Then, using quadratic interpolation (QI), the scale space local maxima (SSLM) of HM is refined and localized. That is, the SURF model instead of utilizing varied measure for choosing the scale and locations [14], the SURF use determinant of HM for scale and location. Let consider a keypoint $X = (x, y)$ for a given image $\mathcal{I}$, the HM $M(X, \sigma)$ in X at scale σ is described using following equation

$$M(X,\sigma) = \begin{bmatrix} \mathbb{L}_{xx}(X,\sigma)\mathbb{L}_{xx}(X,\sigma) \\ \mathbb{L}_{xy}(X,\sigma)\mathbb{L}_{yy}(X,\sigma) \end{bmatrix}, \quad (1)$$

where $\mathbb{L}_{xx}(X,\sigma)$ describes the convolution of Gaussian second order derivatives $\frac{\partial^2}{\partial x^2} g(\sigma)$ considering image I in keypoint $\boldsymbol{X}$ and in similar term for $\mathbb{L}_{xy}(X,\sigma)$ and $\mathbb{L}_{yy}(X,\sigma)$ also it is described. The SSLM of the HM are refined and localized using QI. More details of SURF can be obtained from [13]. The feature set obtained using SURF detector are robust against noise, blurring, scaling, illumination changes, and rotation. Thus, it is significantly used in CMFD. For building efficient CMFD method it is important to good number and distribution of local feature sets. However, in general the SURF based model are very complex with respect to variation of local geometry and illumination changes. Along with, that it provides poor matching performance when compared with the SIFT descriptor. For improving the matching outcome, the SIFT descriptor is used [12].

SIFT features is one of the predominantly used feature extraction technique in the area of image forensics. SIFT features are robust to occlusion, clutter and geometric transformations. A set of SURF keypoints $\mathcal{X} = \{x_1, x_2, x_3 \dots x_n\}$ and their corresponding SIFT descriptors $\{d_1, d_2, d_3 \dots d_n\}$ are extracted from this step and its distance vector $\{v_1, v_2, v_3 \dots v_n\}$ are established using the Euclidian distance (ED) among the x and other $(n-1)$ key point sets. As described in [15], x is matched provided it satisfies condition described in equation(2)

$$\frac{v_1}{v_2} < l \quad (2)$$

where $l \in (0,1)$ depicts user distinct parameter.

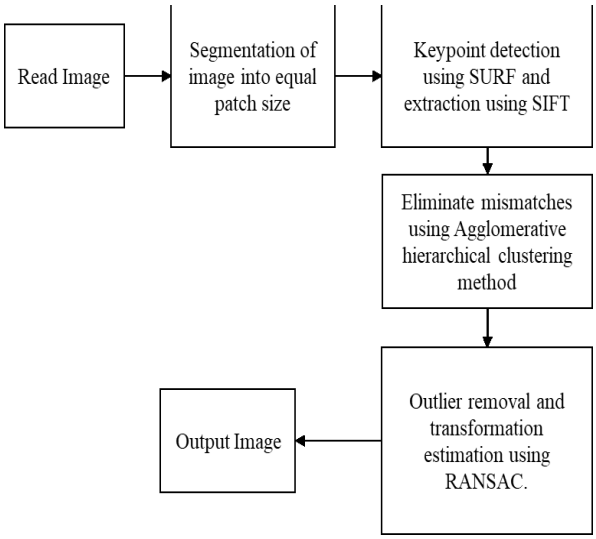


Fig. 1. Block diagram of proposed efficient keypoint based CMFD method.

c) Keypoint matching using hierarchical clustering:

The ideal candidate match of every keypoint x_p is identified by establishing its nearest neighbors (NN) between candidate $n-1$ keypoint sets. This is done by identifying the respective keypoint with the minimal Euclidean Distance (ED) descriptors. By iteratively searching on every keypoint in $\mathcal{X}$, a set of ideal match points is established. Agglomerative hierarchical clustering [15] is employed to improve accuracy of matched points. Clustering helps in deciding whether an area is cloned or not. Then, the reciprocal spatial distances (RSD) between cluster sets is calculated. Closest pair among cluster set is combined into a single cluster. The process is continued in iterative manner till a final merging condition reaches using linkage method and cluster grouping is stopped using threshold $\mathcal{T}_h$. Let consider two cluster $\mathcal{U}$ and $\mathcal{V}$ composed of $n_\mathcal{U}$ and $n_\mathcal{V}$ objects (where $X_{\mathcal{U}i}$ and $X_{\mathcal{V}j}$ depicts the i^{th} and j^{th} objects within cluster $\mathcal{U}$ and $\mathcal{V}$), respectively. The linkage method uses the least ED among objects within two cluster using following equation

$$\mathcal{D}(\mathcal{U},\mathcal{V}) = min\left(\left\|X_{\mathcal{U}i}, X_{\mathcal{V}j}\right\|_2\right) \; with \; i = [1, n_\mathcal{U}], j = [1, n_\mathcal{V}]. \quad (3)$$

In our work the cluster having at least 3 pairs of matching keypoints are said to be cloned.

d) Outlier elimination and image transformation for establishing forged region:

Even though after obtaining matched features still there exist set of mismatches/outlier. Outliers are feature set that is not closer to other feature sets. This work uses RANSAC for eliminating outliers [17]. The RANSAC randomly choose a keypoint sets within the match keypoints and computes the homography. This work considered 3 keypoint pairs. After that, the entire enduring keypoint are transformed based on M and further match using distance metric with associated matched keypoints. Then certain threshold β is defined for determining inlier (i.e., $< \beta$) and outliers (i.e., $> \beta$). Post completing of certain iteration L_{itr}, the transformed output with maximum inlier is selected. This work set L_{itr} to 1000 and β to 0.05. When a test image is identified as tampered, our approach can establish which geometrical transformation (GT) is utilized among the copy-moved segment and original segment. Let's consider the matched feature sets (i.e., point coordinates) of two segments be $\bar{x}_p = (x, y, 1)^G$ and $\bar{x}'' = (x'', y'', 1)^G$, respectively. Their GT association are defined using affine homography, which can be described by a $3 * 3$ matrix M as

$$\begin{pmatrix} x'' \\ y'' \\ 1 \end{pmatrix} = M \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}. \quad (4)$$

This matrix is established considering at least 3 matched keypoints. This work uses maximum likelihood estimation (MLE) of the homography M [16]. The M and efficiently matched keypoints pairs $\bar{x}_p$ and $\bar{x}''_p$ that reduces the cumulated error using following equation

$$\sum_p \left[d\left(x_p, \bar{x}_p\right)^2 + d\left(\bar{x}_p, \bar{x}''_p\right)^2\right] \; subject \; to \; \bar{x}''_p = M\bar{x}_p \forall p. \quad (5)$$

The proposed tampering detection method attain superior performance when compared with existing tampering detection method which is demonstrated experimentally in next section.

III. Experiment Analysis

This section presents performance assessment of proposed EKP-CMFD method over existing CMFD method. The proposed EKP-CMFD method is implemented using Python, C++ and Matlab library and programing language. Experiment is conducted on MICC-F220 dataset which is composed of 220 images out of which 50% are tampered images. Resolution of Images from MICC-F220 dataset varies from 722 × 480 to 800 × 600. More detail of MICC-220 can be obtained from [15], [18], and [21]. The performance of proposed EKP-CMFD and existing CMFD technique are evaluated in terms of following metrics such as True positive rate (TPR) (i.e., recall), False positive rate (FPR), and F1 score. The TPR is evaluated using following equation

$$Recall = \frac{True \; Positives}{True \; Positives + False \; Negatives} \quad (6)$$

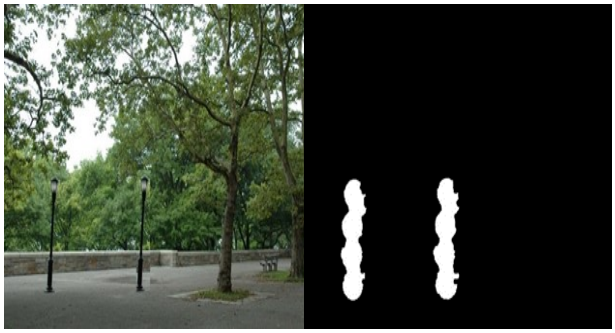
Then, the false positive rate (FPR) is evaluated using following equation

$$FPR = \frac{False\ Positives}{False\ Positives + True\ Negative} \quad (7)$$

Lastly, the F1 score is computed using following equation

$$F1\ score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (8)$$

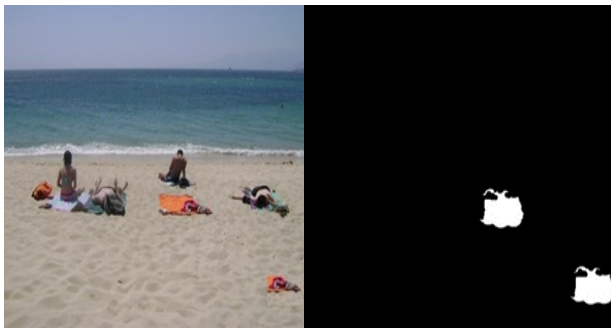
The Fig. 2 shows the sample forgery detection outcome of proposed EKP-CMFD method considering different images. The Fig. 2 (a), (c), (e), and (g) are the original forged images. The Fig. 2 (b), (d), (f), and (h) are the respective forged segment detected image. From result, it can be perceived that the proposed EKP-CMFD method detect and extract forged segment efficiently considering diverse set of images. Fig. 3 shows comparative analysis of proposed EKP-CMDF method over existing CMFD method. The Fig. 3 (a) depicts the original forged image, Fig 3 (b) depicts its corresponding ground truth image, the Fig. 3 (c) depicts the forgery detection outcome attained by SIFT[21] method, Fig. 3 (d) depicts the forgery detection outcome attained by existing method. The Fig. 3 (e) depicts the forgery detection outcome attained by proposed EKF-CMFD. From Fig. 3 (c) it can be observed that SIFT based algorithm fails in detecting forged segment. From Fig. 3 (d) it can be seen the existing model induces few false matches. Thus, from overall result attained, it is noticeable that the proposed EKF-CMFD attain much better forgery detection performance.



(a) (b)

(c) (d)

(e) (f)



(g) (h)

Fig. 2. Output of proposed EKP-CMFD technique

(a) (b)

(c) (d)

(e)

Fig. 3. Comparative analysis of proposed EKP-CMFD over Existing CMFD technique. (a) Input image (b) Ground Truth (c) SIFT (d) Existing method [21] (e) proposed EKP-CMFD

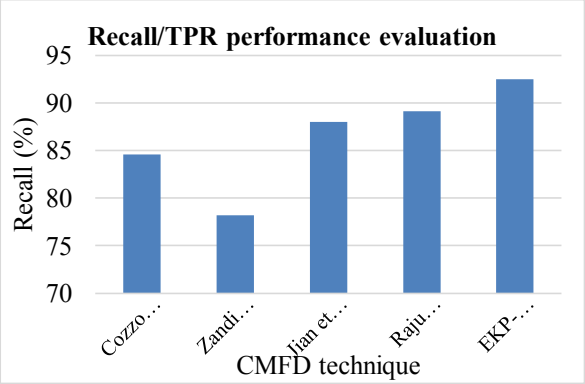


Fig. 4. Recall/TPR performance evaluation of proposed EKP-CMFD over Existing CMFD technique.

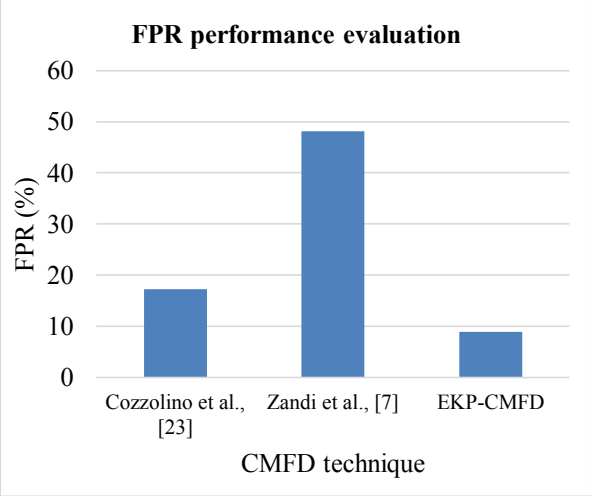


Fig. 5. FPR performance evaluation of proposed EKP-CMFD over Existing CMFD technique.

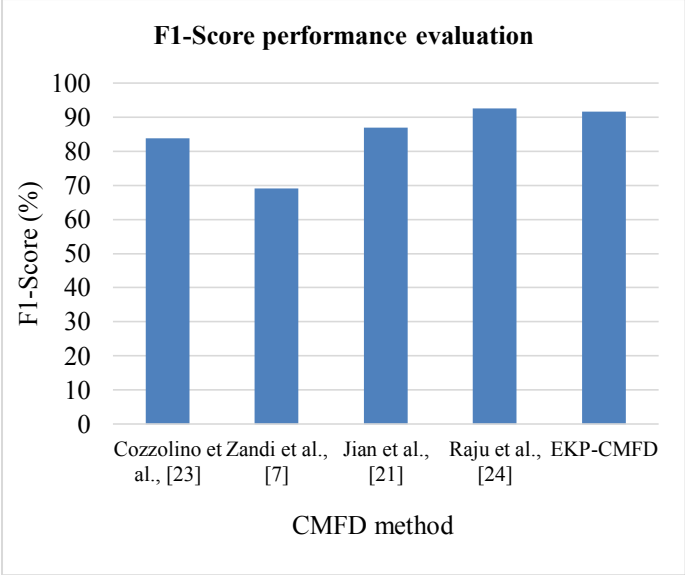


Fig. 6. F1-Score performance evaluation of proposed EKP-CMFD over Existing CMFD techniques.

Table 1: Comparative analysis of EKP-CMFD over existing CMFD techniques

	Recall/TPR	FPR	F1-Score
Cozzolino et al., [23]	84.55	17.27	83.78
Zandi et al., [7]	78.18	48.18	69.08
Jian et al., [21]	88	-	87
Raju et al., [24]	89.14	-	**92.6**
EKP-CMFD	**92.5**	**8.9**	91.7

The table 1, shows the forgery detection performance of EKP-CMFD over various existing method. The Fig. 4 shows recall performance of EKP-CMFD over various existing CMFD method. From results, it is observable that the proposed EKP-CMFD method attain much higher recall performance than other existing CMFD method. The Fig. 5 shows FPR performance of EKP-CMFD over various existing CMFD method. From result, it is evident that the proposed EKP-CMFD method attain much better performance (i.e., lower FPR value) than other existing CMFD method. The Fig. 6 shows F1-score performance of EKP-CMFD over various existing CMFD method. From result it can be seen the proposed EKP-CMFD method attain much higher f1-score performance than other existing CMFD method. From overall result attained it can be seen the EKP-CMFD method attain high classification accuracy with less miss classification of forgery detection.

IV. CONCLUSION

This work first conducted extensive survey of various existing image forgery detection method. From survey it is learnt that copy move forgery is the widely used attack and it is difficult to eliminate. Especially, image forgery under small and smooth region. For detecting CMFD, the block based and key point based method has been used. From extensive study, it is seen that key point based method is much

faster with decent accuracy when compared with block based method. It is important to first obtain optimal number of keypoints even in smooth or small regions. For achieving it, this work presented an efficient keypoint based CMFD method. EKF-CMFD first segmented the image and then applied keypoint based method. Further, this work combined SURF detector with SIFT descriptor for extracting better feature extraction. Further, used agglomerative hierarchical clustering method for feature matching. Then, presented an efficient mismatch elimination and image transformation method using RANSAC. From results it can be seen EKF-CMFD attain a TPR performance of 92.5% which is 3.36% better than existing CMFD model presented by Raju et al. Then, EKF-CMFD attain a FPR performance of 8.9% which is 8.37% better than existing CMFD model presented by Zandi et al. Further, EKF-CMFD attain a F1-score performance of 91.7% which is 0.9% lesser than existing CMFD model presented by Raju et al. From result it is seen the proposed EKF-CMFD model attain significant performance when compared to other existing forgery detection method in terms of recall, FPR, and F1-score. Future work would further consider improving accuracy, reduce false positive with better F1-score by further optimizing EKP-CMFD.

REFERENCES

[1] Y. Ke, Q. Zhang, W. Min, and S. Zhang, "Detecting Image Forgery Based on Noise Estimation,", vol. 9, no. 1, pp. 325–336, 2014

[2] Shivakumar. B. and Baboo.S, "Detection of Region Duplication Forgery in Digital Images Using SURF," International Journal of Computer Science Issues , vol. 8, no. 4, pp. 199–205, 2011.

[3] J. Fan, T. Chen, and J. Cao, "Image tampering detection using noise histogram features," International. Conference on Digit. Signal Process. DSP, vol. 2015-September, pp. 1044–1048, 2015.

[4] J. Zhao and W. Zhao, "Passive Forensics for Region Duplication Image Forgery Based on Harris Feature Points and Local Binary Patterns," Mathematical. Problems in Engineering, vol. 2013, pp. 1–12, 2013.

[5] S. Farooq, M. H. Yousaf, and F. Hussain, "A generic passive image forgery detection scheme using local binary pattern with rich models," Computer and Electrical Engineering, vol. 62, pp. 459–472, 2017

[6] R. Dixit, R. Naskar and S. Mishra,."Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD", in IET Image Processing, vol. 11, no. 5, pp. 301-309, 2017.

[7] Zandi, M.; Mahmoudi-Aznaveh, A.; Talebpour, A. "Iterative copy-move forgery detection based on a new interest point detector". IEEE Transactions on Information Forensics & Security. 11, 2499–2512, 2016.

[8] X. Wang, G. He, C. Tang, Y. Han, and S. Wang, "Keypoints-Based Image Passive Forensics Method for Copy-Move Attacks," International Journal of Pattern Recognition and Artificial Intelligence, vol. 30, no. 3, 2016.

[9] G. Ulutas and G. Muzaffer, "A New Copy Move Forgery Detection Method Resistant to Object Removal with Uniform Background Forgery," Mathematical. Problems in. Engineering, vol. 2016.

[10] Yang, B.; Sun, X.; Guo, H.; Xia, Z.; Chen, X. "A copy-move forgery detection method based on CMFD-SIFT". Multimedia Tools Applications 77,pp. 837–855, 2018.

[11] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copymove forgery detection," IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2284–2297, 2015.

[12] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.

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

[14] Mikolajczyk, K., Schmid, C.," Indexing based on scale invariant interest points". In: ICCV. vol.1, pp. 525 – 531, 2001

[15] 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 TIFS, vol. 6, no. 3, 2011.

[16] R. I. Hartley and A. Zisserman, Multiple View Geometry in Computer Vision. Cambridge, U.K.: Cambridge University Press, 2004.

[17] M. Fischler and R. Bolles, "Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography," Communication. ACM, vol. 24, no. 6, pp. 381–395, 1981.

[18] I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo, D. Tongo, G. Serra, "Copy-move forgery detection and localization by means of robust clustering with Jlinkage". Signal Process. Image Communication 28(6), pp. 659–669,2013

[19] E. Silva, T. Carvalho, A. Ferreira, A. Rocha, "Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes". Journal of Visual Communication and Image Representation. 29, pp. 16–32,2015

[20] C.M. Pun, X.C. Yuan, X.L. Bi, "Image forgery detection using adaptive over segmentation and feature points matching". IEEE Transactions on Information Forensics and Security 10(8), pp.1705–1716, 2015

[21] J. Li, X. Li, B. Yang, X. Sun, "Segmentation-based image copy-move forgery detection scheme". IEEE Transactions on Information Forensics and Security. 10(3), pp.507–518, 2015.

[22] Huang, Hui-Yu & Ciou, Ai-Jhen, "Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation", EURASIP Journal on Image and Video Processing. 2019.

[23] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copymove forgery detection," IEEE Transaction on Information Forensics and Security, vol. 10, no. 11, pp. 2284–2297, 2015.

[24] Raju, P.M., Nair, M.S.: "Copy-move forgery detection using binary discriminant features". Journal of King Saud University. – Computer and Information Sciences, 2018.