Journal of Engineering Science and Technology
Vol. 16, No. 2 (2021) 1525 - 1538
© School of Engineering, Taylor's University

PROPOSED IMAGE FORGERY DETECTION METHOD USING IMPORTANT FEATURES MATCHING TECHNIQUE

EKHLAS WATTAN GHINDAWI[1,*],
SALLY ALI ABDULATEEF[1], LAMYAA MOHAMMED KADHIM[2]

[1]Computer Science Department, University of Al-Mustansirihya, Baghdad, Iraq
[2]College of Dentistry, University of Al-Mustansirihya, Baghdad, Iraq
[*]Corresponding Author: watanikhlas@gmail.com

Abstract

The copy-move forgery might be specified as frequently applied manipulation approach for the purpose of tampering the digital images. Key-point based detection methods have been effective in revealing the copy-move evidence, due to the fact that they are robust against a lot of attacks, including wide scale transformation's geometrical types. Yet, such methods showed no success to handle conditions in which copy-move forgeries just including smooth or small areas, in which there is limited number of key-points. To handle such problem, this work suggested rapid and efficient algorithm to detect copy-move forgeries through hierarchical feature point matching. Then, novel matching approach was designed to solve issues related to key-point matching over various key-points. To reduce false alarm rate as well as areas' accurate localization which were subjected to tampering, the study suggested a method of localization via using the robustness's properties (that involve dominant orientation and scale information). Thorough experimental results were made available to show the efficient performance related to the proposed approach, on the basis of efficiency and accuracy.

Keywords: Copy-move forgery, Forgery detection, Iterative localization, Hierarchical feature matching.

1. Introduction

As the up-to-date editing software (such as Gimp and Photoshop) are developed rapidly, digital image might be forged at extremely reduced costs. This is going to cause huge threats to the digital image's reliability. Also, the copy-move forgeries have been frequent manipulation approach, in which single or a few image regions have been pasted in other location of the image for the purpose of duplication or hiding objects of interest [1-7]. The approach might be used with noise addition, resizing, rotation, and compression for making the last forgery more efficient. Often, there is extreme challenge to detect them, particularly in the case when copy-move forgeries just involve smooth or small regions, or in the case when forged areas were subjected to processing via extreme attacks, like heavy noise addition and large-scale resizing, some examples can be seen in the Fig. 1, in which copy-move forgery has been carried out over just the small or smooth regions.

Recently, a lot of the approaches to detect image copy-move forgery were suggested, that might be specified into 2 groups: 1) dense-field (or block-based) methods [1, 2, 6, 8-13] and 2) sparse-field (or key point-based) methods [3, 5, 14-21]. With regard to the former, input images will be initially divided to regular and overlapped blocks; after that, the process of forgery localization will be achieved via block matching.

This work suggested rapid and efficient algorithm to detect copy-move forgeries through hierarchical feature point matching. Then, novel matching approach was designed to solve issues related to key-point matching over various key-points. To reduce false alarm rate as well as areas' accurate localization which were subjected to tampering, the study suggested a method of localization via using the robustness's properties.

In the following sections the proposed method will be presented in detail , Section 2 views the related works, Section 3 explains the proposed system in three sub sections, Section 4 shows the experimental result in three tests, and Section 5 views the conclusions.

Fig. 1. An example of the copy-move forgery.

2. Related Works

For the purpose of enhancing the robustness against a few known distortions, like geometric transformations, a lot of approaches were used for designing block features, including such as Discrete Cosine Transform (DCT) [1], Discrete Wavelet Transform

(DWT) [2], Principal Component analysed (PCA) [8], Singular Value Decomposition (SVD) [9], in addition to other methods [10, 11]. Dense-filed methods have high accuracy in comparison to sparse-field ones at the cost of high complexity [6].

Lately, a study conducted by Cozzolino et al. [12] suggested effective block-based copy-move forgery detection technique, in which processing time has been decreased via resorting to PatchMatch algorithm, which is considered as rapid approximate nearest-neighbour search approach [22].Regrettably, all present block-based approaches are suffering from several attacks, like noise addition, rotation, and scaling.

A study conducted by Pan et al. [14] used key-point matching for providing robustness against copy-move forgeries. With the use of Scale Invariant Feature Transform (SIFT) feature [23], the approach had high robustness against geometric transformations, in which parameters have been evaluated via RANdom SAmple Consensus (RANSAC) algorithm [24]. Comparable system has been suggested via Amerini et al. [3] for detecting multiple duplicated regions, in which matched correspondences might be following distinctive geometric transformations. With regard to such condition, RANSAC estimation through all matched pairs will not work anymore.

For handling such problem, [3] indicated using hierarchical agglomerative clustering algorithm [25] for grouping matched key-points to separated clusters on the basis of their location in image plane, after that applying RANSAC estimation throughout each two matching clusters. Instead of key point's clustering, the best current solution proposed by Amerini [16] suggested clustering matching pairs in conceptual space. In brief, this work referred to these key point-based approaches that involve clustering processes as the key point-clustering-based algorithms.

Rather that applying clustering algorithms for grouping matched key points, other studies suggested initially segmenting the image to small and non-overlapped patches; the process of matching has been carried out between each two segmented regions [5]. Key point-based copy-move forgery detection approaches were examined from many aspects, they had less accuracy in comparison to dense-field approaches [6, 12].

3. Proposed System

The presented study is providing accurate and effective key point-based approach for detection and localization of the image copy-move forgeries, offering excellent performance even in the case when such forgeries involving small or smooth regions, or in the case when forged images were processed via certain attacks (for example, heavy noise addition and large-scale resizing). Figure 2 presents a framework related to the suggested scheme of image forgery detection that follow classic workflow, such as:

- Important feature extraction stage
- Correct matches stage
- Forgery localization stage.

3.1. Important features extraction (FS) stage

Features extraction stage or FS is essential for all systems requiring matching. Obtained features might be separated in feature space for producing efficient distinguishing between the images. The suggested approach is focusing to extract important features. Utilizing important features in the process of forgery detection might be satisfying accurate and rapid matching [26-28], also it will result in precise estimation related to the transformation parameters [27, 28]. For the purpose of finding image's important features, the approach is extracting corners as major features, with the use of Harris Corner Detector for producing feature set as initial stage.

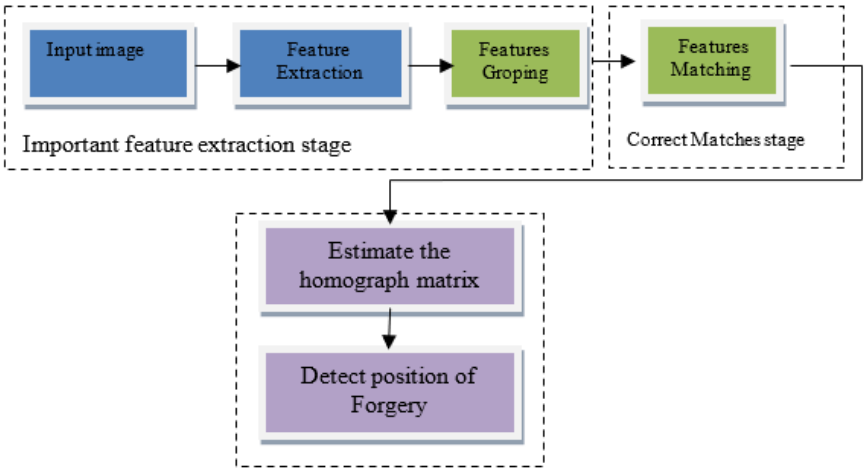

Fig. 2. The proposed method diagram.

Regarding the second stage, the feature set is going to be divided into groups of associated features. Various interest point detectors were suggested and utilized based on application. Robust, fast, and rotation invariant, Harris detector has been utilized in a lot of applications related to computer vision that applies auto-correlation function for determining locations in which signal changes in 1 or 2 directions. The suggested approach is selecting corners as optimum features which will be extracted, due to the fact that corner has been considered as meeting point related to the two edges, in which it is representing point related to change the direction of edges, also corners have extra stable features over the modifications in viewpoints [29-31]. Furthermore, corners have been excellent feature for matching due to its large variations in neighbourhood related to point in all the directions. Also, Harris Corner Detector was utilized for extracting corner features from the frame of video. The effectiveness of Harris Corner Detector specified via its capability for detecting the same corners in the images within different lighting conditions as well as geometric transformations like rotation and translation [32-35]. To extract corner features from image has been the initial stage, the other stage is to detect important features from feature set. Furthermore, group features suggest determining the significance of features, even though that affiliation related to such feature to group.

The major approach is to gather features set in single group and consider each one of the features in group as important feature. In the case when grouping the

features on the basis of minimum distances, indicating that such set of features are belonging to important region, also it has an impact on the details of image and of high importance in the accuracy of forgery detection. Feature's grouping on the basis of minimal distance as three benefits:

- Group the features ignore related to features and determining relevant ones.
- Dependence on the wrong features might result in decrease of registration accuracy or quality as well as unnecessary elevation in the computational costs, also the time needed for performing the important.
- The process of grouping will be increasing the feature matches' reliability.

For the purpose of obtaining precise detection related to important features, the selection of three features has been conducted. Each one of the three features will be gathered in single group on the basis of its locations and on the basis of achieving minimum distance.

3.2. Correct matches stage

Following the extraction of important features, correct matches should be specified. This approach is based on a system related to search in neighbours with regard to each one of important features, also incorporating some tests for ensuring accuracy. Certain approach is used for detecting and ignoring false as well as repeated matches. For increasing the reliability and validity related to matched features, the suggested approach uses only the centroid related to each one of important feature groups regarding initial image for searching the correct matches in all the second image's important features. With regard to each one of the centroid important features (F) in first image, search area is going to be specified in the other image, involving features in same location, also the 8-neighbors.

This approach is searching for all the important features in specified area and finding match feature, based on satisfying minimum distance to the feature F. This process applies features vector which is acquired from the former stage (Harris corner detector), also the output related to the process has been set of centroids applied as input to the following stage. The presented study comes with the aim of providing contributions for determining correspondence between two images. It is helping in the automatic FS. Besides the high performance related to registration approach through limiting to few features decreased at same time the complexity related to the approach. Also, this is helping for betting interpreting the results. Following specifying the local groups in 2 images, point-matching system should be carried out for finding comparable points in 2 images via estimating the groups. As soon as being matched, they will be indicated as point correspondences. The matches have been verified through determining distance or similarity measure.

Real implementations related to this system must assess similarity or distance marl related to each one of interest points in single image against each one of interesting points in the second image. The bad pairs will be eliminated, while the good pairs will be selected following checking optimum match against the other match marks with regard to each set of correspondences. The feature satisfies the minimum distance, but it is not matched feature, that is called false matches. One way to find the true and false matches is by using a threshold where the distance of true matches must be smaller than a specific threshold value T. To determine the threshold value, which detect the false matches, the proposed work suggests a

method to detect the threshold value .The threshold value is the average value of all distances from the feature F and all-important features in the 8-nieghberhood area. The refuse of couples related to pixels have been carried out on pixels with distance from other has been more than certain threshold.

3.3. Forgery localization

With regard to this section, iterative localization approach will be suggested without including segmentation and clustering processes. The suggested system is developed via totally adopting robustness properties (involving scale information and dominant orientation), also the colour information related to each of the matched key points. The suggested system will be achieving elevated accuracy regarding forgery localization. The framework related to the suggested forgery localization approach can be seen in Fig. 2 (stage 3). Generally, the presented approach includes two steps:

Step 1): Estimating local homography.

Step 2): Forgery localization with the use of scale as well as colour information.

Step 1.Estimating local homography:

RANSAC algorithm can be used for estimating the homography Hk between correspondences regarding matched pairs. The affine matrix will be estimated with the use of all matched pairs from 2 contiguous local regions that is going to be more refined with the use of inliers.

Step 2. Forgery localization:

This step will be generating the detected forgery regions through sequentially using the next 2 processes on the original image: 1) removing the small regions; also 2) filling the small gaps via morphological close operation. The image will be specified as original in the case when all original image's elements are 0; or else it will be specified as forged image.

4. Experimental Results

The suggested approach was carried out with the use of Matlab-13 in a PC with memory 4GB and CPU 2.60 GHz. Fast Harris detector along utilized for detecting the interest points. The major task in all object recognition has been to match the similarity between two feature points. Images that have been chosen will be collected.

Due to the fact that the image's size is of high importance, there is requirement for detection algorithms, there are 6 distinctive images specified for being more difficult for the detection of copy-move forgery with different size and resolution related to copied area utilized in this study. The images have been selected from the dataset proposed in [35]. The resolution was high in three images (over 2000×1600) pixels, also three images with low resolutions. Furthermore, copied region is of the same appearance related to original image, thus, the key points that are extracted in duplicated region is going to be comparable to original ones. Thus, the matching in features might be used for the task to determine the potential tampering. This study will be reporting certain experimental results on the images in which copy-move attacks were achieved.

Regarding such condition, the forged region is going to be chosen on the basis of certain goal that will be satisfied, also focusing on effectively concealing modification, in which alterations have not been recognizable at least at first glance as well as the forensic tool might be helping in investigations.

4.1. Test one

With regard to the suggested Harris threshold will be set for 300 for the images of high resolution, also 50 for the images of low resolution. Initially, the suggested approach has been analysed for determining optimum setting for cut-off threshold T_h (matching) related to images. Also, through reduction in Harris threshold, there will be an increase in key-points, that lead to more match points and thus increasing the detection duration. The results are indicating that the suggested approach is effectively detecting the copy-move forgeries. Figure 3 shows high-resolution tampered images (top row), key-points that are obtained for tampered images (middle row) as well as detection result (bottom row).

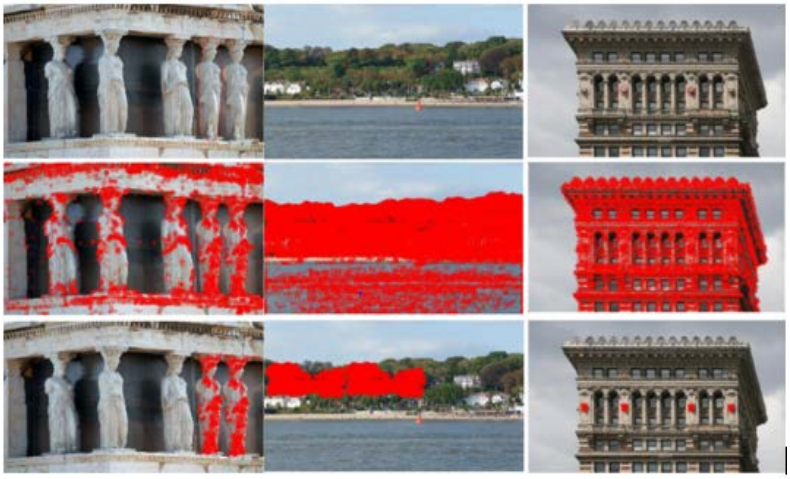

Fig. 3. a) Forged images have been in top row. Forged area has been highlighted by ellipse or circle. b) Key points obtained for the tampered images have been specified in middle row. c) The last row showing the detected area.

Table 1 is showing optimum matching threshold regarding each of the images, the number of the key-points extracted as well as detection time (in seconds) have been indicated for the 3 high-resolution images.

Table 1. Optimum threshold (matching).

Image	Threshold (T_h)	No. of Keypoints	Matches	Detection Time (s)
Acropolis	**0.14**	**5300**	**1100**	**957.00**
Beachwood	**0.07**	**18500**	**4200**	**1297.150**
Building	**0.10**	**9450**	**100**	**2690.070**

For analysing the suggested approach's performance, experiment has been indicated with the low -resolution images. This is considered as a situation of high

importance to forged region's individuation in the image indicated as Giraffe and Tree, the approach has the ability for detecting adequate number of the matched key-points. At the same time, regarding an image referred to as Cattle, in which 2 regions have been forged, the approach has the ability for detecting just single forged region for certain Harris threshold (300). This has been majorly because of the smaller number of extracted key-points. Thus, this work decreased Harris threshold to 50, for having adequate number of key-points for images of low-resolution. Furthermore, the results are indicating the suggested approach is detecting forged region effectively for low-resolution images, in the case when there have been more key points. With regard to Table 2, the number of extracted key-points, also the detection time (sec.) in addition to optimal matching threshold for every one of the images have been indicated. Figure 4 illustrates the forged areas in some details .

Table 2. Optimum threshold (matching).

Image	Threshold (T_h)	No. of Keypoints	Matches	Detection Time (s)
Cattle	**0.09**	**4470**	**57**	**645.0**
Tree	**0.15**	**2300**	**40**	**230.700**
Giraffe	**0.10**	**2250**	**40**	**188.800**

Fig. 4. a) Forged images are in the top row. The forged area was highlighted by circle or ellipse. b) The key-points which have been obtained for the tampered images are illustrated in the middle row. c) The bottom row illustrates the detected area. From left to right: Cattle (2 small, copied areas), Tree (large, copied area) and Giraffe (small, forged area).

4.2. Test two

The suggested approach has been analysed as well for the determination of the efficiency of the tampered images having several copies of one area. For the sake of addressing this issue, 2 high resolution Acropolis images and low-resolution Tree image has been used. The rightmost statues in Acropolis image and the tree in Tree image have been copied and then pasted in a number of various places in the original image. Figure 5 illustrates the result of the detection which has been obtained with several copied areas respectively for the Acropolis and Tree images. The results that show in Table 3, illustrate the number of the obtained key-points, the amount of the key-points was matching and the time of the detection for the Acropolis image following multiple forgeries.

Fig. 5. Examples of the altered images (i.e., Acropolis) with several copying instances have been illustrated in 1st row and the results of the detection have been shown in the 2nd row.

Table 3. Number of the obtained key-points, the amount of the key-points was matching and the time of the detection for the Acropolis image following multiple forgeries.

No. of forgeries	No. of key points	Matches	Detection time (s)
1	5,339	1,114	957.8730
2	6,034	1,760	1109.3660
3	6,687	2,388	1102.7530
4	7,378	3,017	1382.9030

It should be noted that the amount of the key-points as well as the amount of the matched points increased in a proportional way for Acropolis image, where image lighting was constant over the image. In contrast, for the Tree with several forgeries, the amount of the matched points had no proportional increase due to the fact that the image is not flat, and the illumination distributed over the image is not similar. Figure 6 shows some examples of the images that have been tampered (i.e., Tree) with several copying processes have been illustrated in 1st row and the results of the detection have been shown in the 2nd row and Table 4 illustrates the number of the

obtained key-points, the number of the key-points which have been matched and the time of the detection for the tree image following multiple forgeries.

Table 4. The number of the obtained key-points, the number of the key-points which have been matched and the time of the detection for the tree image following multiple forgeries.

No. of forgeries	No. of key-points	Matches	Detection time (s)
1	2,274	37	242.5170
2	2,788	39	228.790
3	2,800	80	232.2050
4	2,803	98	225.8510

Fig. 6. Examples of the images that have been tampered (i.e., Tree) with several copying processes have been illustrated in 1st row and the results of the detection have been shown in the 2nd row.

4.3. Test three

The present section analyses the efficiency of the proposed system for testing the images that have been transformed. Images which have been forged are produced in the Acropolis image for which the scaling (i.e., symmetric or asymmetric) has been implemented. Table 5 summarizes geometrical transformation types for attack which is applied on the cloned part in Acropolis image. For instance, in attack F, x and y axes undergo a 20% scaling. Figure 7 shows the results of the detection for a variety of the scaling positions in details

Table 5. Variety of the geometrical transformation (scaling) combinations which have been implemented on the Acropolis image.

Attacks	Sx	Sy	No. of key-points	Matches points	Detection time (s)
a	1.0	1.1	5,340	714	1001.0840
b	1.1	1.0	5,416	742	1335.7340
c	1.1	1.1	5,379	487	991.9710
d	1.0	1.2	5,300	271	1040.2910

e	1.2	1.01.2	5,399	229	1107.0520
f	1.2	1.2	5,296	91	1020.9440
g	1.0	0.9	5,416	620	899.0590
h	0.9	1.0	5,376	658	973.5040
i	0.9	0.9	5,404	391	955.9990
j	1.0	0.8	5,434	125	955.4400
k	0.8	1.0	5,346	77	1278.1950
l	0.8	0.8	5,380	15	1405.9640

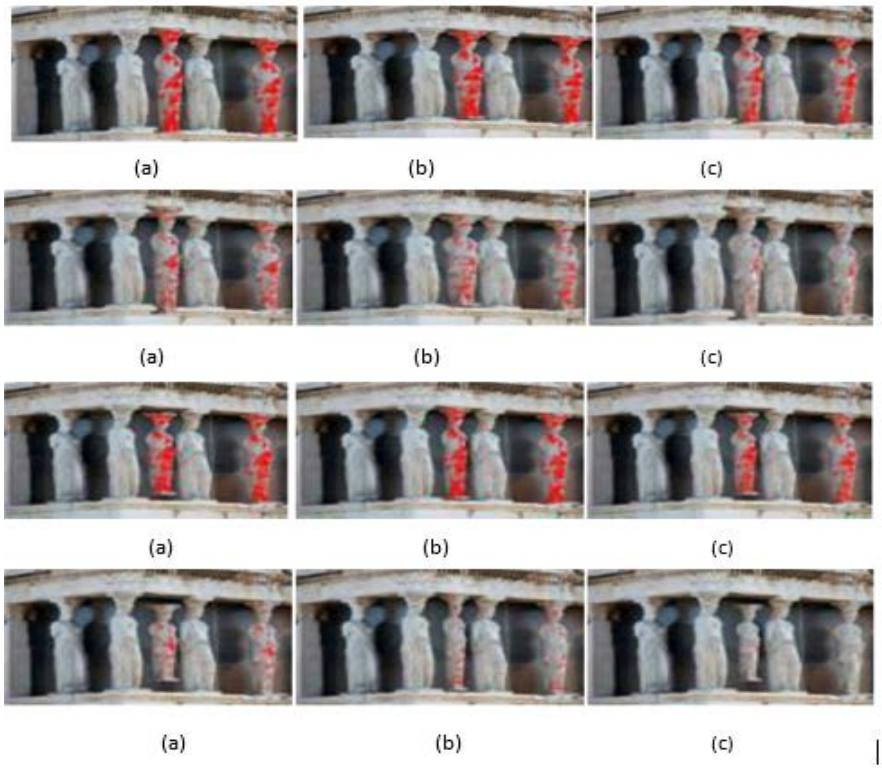

Fig. 7. The results of the detection for a variety of the scaling positions.

5. Conclusion

A method for supporting the research of the image forensics according to the Harris interest point was suggested. Taking under consideration a suspected image with the high and the low resolutions, this system has the ability of the reliable detection in the case of the duplication of a specific region in the image. Initially, it has been shown that there is a possibility in generating an adequate amount of the key-points even in the small or smooth areas. Afterwards, an innovative strategy of the hierarchical feature point matching was suggested for alleviating the tasks of the critical matching. For the reduction of the rate of the false alarms in addition to the accurate localization of copied areas, we additionally suggested a method of localization without the involvement of any processes of segmentation or clustering. The suggested methodology accomplishes a considerably high accuracy of the detection. The detailed experimental results were given for demonstrating the better performance of the suggested approach. In addition to that, this method

has the ability of the effective detection of the tampered images that have been transformed like scaling. None-the-less, this system has shown weakness in the detection of the images that have been undergone some attacks like the Gaussian noise and rotation. In future, the aim is dealing with some of those issues.

References

1. Fridrich, A.J.; Soukal, B.D.; and Luka´s, A.J. (2003). Detection of copy-move forgery in digital images. *Proceedings of. Digital Forensic Research Workshop*.
2. Muhammad, G.; Hussain, M.; and Bebis, G. (2012).Passive copy move image forgery detection using undecimated dyadic wavelet transform. *Digital Investigation*, 9(1), 49-57.
3. Amerini, I.; Ballan, L.; Caldelli, R.; Del-Bimbo, A.; and Serra, G. (2011). A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security*, 6(3), 1099-1110.
4. Li, Y.; Zhou, J.; Cheng, A.; Liu, X.; and Tang, Y.Y. (2016). SIFT keypoint removal and injection via convex relaxation. *IEEE Transactions on Information Forensics and Security*, 11(8), 1722-1735.
5. Li, J.; Li, X.; Yang, B.; and Sun, X. (2014). Segmentation-based image copy-move forgery detection scheme. *IEEE Transactions on Information Forensics and Security*, 10(3), 507-518.
6. Christlein, V.; Riess, C.; Jordan, J.; Riess, C.; and Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on Information Forensics and Security*, 7(6), 1841-1854.
7. Li, Y.; Zhou, J.; and Cheng, A. (2017). SIFT keypoint removal via directed graph construction for color images. *IEEE Transactions on Information Forensics and Security*, 12(12), 2971-2985.
8. Popescu, A.C.; and Farid, H. (2004), *Exposing digital forgeries by detecting duplicated image regions.*, (TR2004-515), Dartmouth College, Hanover, US.
9. Zhao, J.; and Guo, J. (2013). Passive forensics for copy-move image forgery using a method based on DCT and SVD. *Forensic Science International*, 233(1-3), 158-166.
10. Bayram, S.; Sencar, H.T.; and Memon, N. (2009). An efficient and robust method for detecting copy-move forgery. *IEEE International Conference Acoustics, Speech and Signal Processing*, 1053-1056.
11. Ryu, Seung-Jin. ; Kirchner, M.; Lee, Min-Jeong.; and Lee, Heung-Kyu. (2013). Rotation invariant localization of duplicated image regions based on zernike moments. *IEEE Transactions on Information Forensics and Security*, 8(8), 1355-1370.
12. Cozzolino, D.; Poggi, G.; and Verdoliva, L. (2015). Efficient dense-field copy-move forgery detection. *IEEE Transactions on Information Forensics and Security*, 10(11), 2284-2297.
13. Xiuli, B.; and Pun, Shi-Man. (2017). Fast reflective offset-guided searching method for copy-move forgery detection. *Information Sciences*, 418-419, 531-545.

14. Pan, X.; and Lyu, S. (2010). Region duplication detection using image feature matching. *IEEE Transactions on Information Forensics and Security*, 5(4), 857-867.
15. Silva, E.; Carvalho, T.; Ferreira, A.; and Rocha, A. (2015). 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, 16-32.
16. Amerini, I.; Ballan, L.; Caldelli, R.; Del-Bimbo, A. ; Del-Tongo, L.; and Serra, G. (2013). Copy-move forgery detection and localization by means of robust clustering with j-linkage. *Signal Processing: Image Communication*, 28(6),659 -669.
17. Meena, K.B..; and Tyagi, V. (2019). Image Forgery Detection: Surveyand Future Directions. *Data, Engineering and Applications*, 163-194.
18. Zhang, Z.; Wang, C.; and Zhou, X. (2018). A survey on passive image copy-move forgery detection. *Journal of Information Processing Systems*. 14(1), 6-31.
19. Guo, Jing-Ming.; Liu,Yun-Fu.; and Wu, Zong-Jhe. (2013). Duplication forgery detection using improved DAISY descriptor. *Expert Systems with Applications*, 40(2), 700-714.
20. Kakar, P.; and Sudha, N. (2012). Exposing postprocessed copy-paste forgeries through transform-invariant features. *IEEE Transactions on Information Forensics and Security*, 7(3), 1018-1028.
21. Li, Y.; and Zhou, J. (2018). Image copy-move forgery detection using hierarchi-cal feature point matching. *IEEE Transactions on Information Forensics and Security*, 14(5), 1-4.
22. Barnes, C.; Shechtman, E.; Finkelstein, A.; and Goldman, D.B. (2009). Patchmatch: A randomized correspondence algorithm for structural image editing. *ACM Transactions on Graphics*, 28(3), 1-11.
23. Lowe, D.G. (2004). Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 60, 91-110.
24. Fischler, M.A.; and Bolles, R.C. (1981). Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*, 24(6), 381-395.
25. Friedman, J., Hastie, T.; and Tibshirani, R.; and (2009). *The Elements of Statistical Learning*. New York: Springer.
26. Mikolajczyk, K.; and Schmid, C. (2005). A performance evaluation of local descriptors. *IEEE Transactions Pattern Analysis and Machine Intelligence*, 27(10), 1615-1630
27. Qin, Z.; Yan, J.; Ren, K.; Chen, and C.W. (2014). Towards efficient privacy-preserving image feature extraction in cloud computing. Proceedings of International Conference on Multimedia, 497-506.
28. Cozzolino, D.; Poggi, G.;and L. Verdoliva.(2014). Copy-move forgery detection based on patchmatch. *IEEE International Conference on Image Processing*, 5312-5316.
29. Vedaldi, A.; and Fulkerson, B. (2008). VLFeat: An open and portable library of computer vision algorithms. *Proceedings International on Multimedia*, 1469-1472.

30. Hartley, R.; and Zisserman, A. (2003). *Multiple view geometry in computer vision*. New York: Cambridge university press.
31. Bravo-Solorio, S.; and Nandi, A.K. (2011). Exposing duplicated regions affected by reflection, rotation and scaling. *IEEE International Conference on Acoustics, Speech Signal Processing*, 1880-1883.
32. Zandi, M.; Mahmoudi-Aznaveh, A.; and Talebpour, A. (2016). Iterative copy-move forgery detection based on a new interest point detector. *IEEE Transactions on Information Forensics and Security*, 11(11), 2499-2512.
33. Vandewalle, P.; Kovacevic, J.; and Vetterli, M. (2009). Reproducible research in signal processing. *IEEE Signal Processing Magazine*, 26(3), 37-47.
34. Wen, B.; Zhu, Y.; Subramanian, R.; Ng, T.; Shen, X.; and Winkler, S. (2016). COVERAGE - a novel database for copy-move forgery detection. *IEEE International Conference on Image Processing*, 161-165.
35. Christlein. V.; Riess. C.; and Angelopoulou. E. (2010). A Study on Features for the Detection of Copy -Move forgeries, in GI SICHERHEIT.