2021 5th International Conference on Pattern Recognition and Image Analysis (IPRIA)
Department of Electrical and Computer Engineering, University of Kashan, Iran, 28 & 29 April 2021

Discriminating the Original Region from the Duplicated in Copy-Move Forgery

Saba Salehi
Cyberspace Research Inst.
Shahid Beheshti University
Tehran, Iran
s.salehi0026@gmail.com

Ahmad Mahmoodi-Aznaveh
Cyberspace Research Inst.
Shahid Beheshti University
Tehran, Iran
a_mahmoudi@sbu.ac.ir

2021 5th International Conference on Pattern Recognition and Image Analysis (IPRIA) | 978-1-6654-2659-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/IPRIA53572.2021.9483497

***Abstract*—Since images are used as evidence in many cases, validation of digital images is essential. Copy-move forgery is a special kind of manipulation in which some parts of an image is copied and pasted into other parts of the same image. Various methods, proposed to detect copy-move forgery, have achieved promising results. In previous methods, a binary mask determining the original and forged region is presented as the final result. However, it is not usually specified which part of the mask is the forged region. It should be noted that discriminating the original region from the duplicated one is not usually feasible by human visual system (HVS). On the other hand, exact localization of the forged region can be helpful for automatic forgery detection especially in combined forgeries. In real-world forgeries, some manipulations are performed in order to provide a visibly realistic scene. These modifications are usually applied on the boundary of the duplicated snippets. In this research, the texture information of the border regions of both the original and copied patches have been statistically investigated. Based on this analysis, we propose a method to discriminate the copied snippets from the original ones. In order to validate our method, several benchmark datasets are employed.**

Keywords*— *image forgery detection, copy-move forgery, image texture analysis, local binary patterns

I. INTRODUCTION

With the development of advanced image editing software, image forging can be performed easily. Since the images are usually used as evidence, the authentication of digital images is important. Manipulation detection methods are divided into active and passive approaches. The active approach, including digital signature and digital watermarking, requires extra information to detect manipulations. Therefore, they could not be used in all applications. Consequently, the passive approach was proposed, which mainly seeks to find out the statistical inconsistency in natural images.

Image manipulation can be generally classified into three types [1], image retouching, image splicing, and copy-move forgery. Image retouching, improves image appearance such as contrast, is the least harmful kind of manipulation. A forged image is created by combining more than two images in splicing. In copy-move forgery, some snippets of an image are copied and pasted into other parts of the same image. This forgery is usually used to hide an object or increase the number of objects for exaggeration in the image.

Splicing may introduce inconsistencies in image characteristics; hence, splicing detection methods are mostly based on analyzing the inconsistencies among local features. Since in copy-move forgery copied regions are part of the original image, it is not feasible to employ splicing detection methods to such images. Copy-move forgery detection methods are based on finding similarity in an image.

Numerous methods have been proposed to detect copy-move forgery. Some of them present impressive results. However, the majority of them do not discriminate the original and forged region. They generally provide a binary mask, containing the original and duplicated regions. In this paper, we present a method which can distinguish the original patches from the forged ones. It should be noted that it is a challenging task due to the similarity of image properties in the original and the duplicated regions.

This paper is organized as follows: In section II, a review of forgery detection methods is presented. We will examine the proposed method in section III. The proposed method is evaluated in section IV. Finally, we clarify our conclusion.

II. REVIEW OF PASSIVE DETECTION APPROACH

The most common way of manipulating images is splicing forgery. It is combines two (or more) images to create tampered images. Forgery detection methods are mostly based on inconsistency in image characteristics. As a case in point, photos captured by different digital cameras usually have different noise pattern. In this case, forged images which are created with the different cameras can be detected by investigating the noise [2]. Another technique for splicing forgery detection is performed by analyzing the amount and types of blurriness, such as motion and out-of-focus blur [3].

In copy-move forgery, one or more image regions are copied and pasted in another region of the same image. Since the copied one is from the original image itself, some image properties, such as noise, are identical in the original and copied region. Therefore, methods used to detect splicing forgery are not usable in copy-move forgery. The main approach for

978-1-6654-2659-6/21/$31.00 ©2021 IEEE

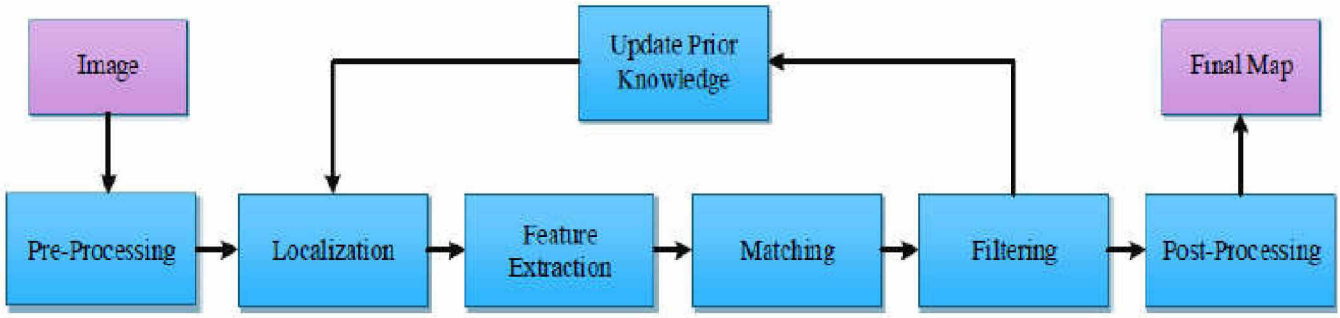

FIG 1. COMMON FRAMEWORK OF THE COPY-MOVE FORGERY DETECTION METHODS [4]

detecting copy-move forgery is to identify similar regions. To detect this kind of forgery, several methods have been proposed, which follow a general framework that is shown in Fig.1.

There are some preprocessing phases in the first step to facilitate the next steps. Converting color image to grayscale is one of them. The second step is localization. This step can be implemented with two approaches: block-based and keypoint-based. The block-based approach divides the image into overlapping blocks, and all possible blocks are extracted. In keypoint-based approach, merely high entropy regions, i.e. keypoints are just explored. In the feature extraction step, features are extracted from each block or keypoint, using a descriptor. Afterward, a feature vector is obtained. Feature vectors are compared to find similar blocks. Due to self-similarity property of natural images, a number of similar blocks will be detected incorrectly. In the next step, the matched pairs are filtered to remove the blocks that are incorrectly matched. In the phase of updating information, some methods repeat some previous steps in order to more precisely localize forged regions. Postprocessing steps are also used to make the output more accurate. The resultant output in copy-move forgery detection methods, is a binary mask in which the forged region is not discerned from the original one.

The first method by Friedrich et al. [5] was proposed to detect copy-move forgery. First, they examine all of the overlapping image blocks. Then, discrete cosine transform (DCT) is used for describing the overlapped blocks. The features extracted from each block are lexicographically arranged. Then, the similar blocks are found by comparing their description. Since the truly matched pairs have a same shift vector, falsely matched pairs can be removed on this basis.. Other block-based methods work likewise in general, but with some modifications. For example, in feature extraction, they use rotation invariant transforms [6],[7] or some methods use hashing -based matching algorithms such as LSH [6], [7]. Another approach is to use improved filtering algorithms [6], [7].

Block-based methods have heavy computations because all image blocks are considered. Hence, keypoints-based methods have been introduced, which would greatly reduce the computational cost. The two common ways in this regard are SIFT and SURF. The first keypoint-based methods [8], [9] use SIFT to extract and describe keypoints. For matching, instead of using the similarity of two feature vectors, the ratio between the nearest neighbor to the second nearest neighbor is used. The challenge of keypoint-based methods is to identify smooth regions that have been tampered. It is due to the fact that sufficient keypoints are not extracted from such regions.

There are other approaches to detect copy-move forgery. A method is proposed in [10] and [11], which divides the image into non-overlapping semantic parts and then extracts keypoints from the entire image which are matched afterwards. Two regions are identified as matched, if they have a certain ratio of the matched keypoints. Moreover, the original and copied region should not be in the same region.

The PatchMatch algorithm introduced in 2009 [12] is a randomized algorithm that searches the entire image randomly to find the closest neighbor. Also, this algorithm has been used to detect copy-move forgery [13]. This method has less computational complexity due to the utilization of a random search algorithm.

Considering the fact that the employed keypoint extraction methods are not designed for copy-move detection, in [4], a new method for extracting keypoints is proposed. In this way, even smooth regions are covered in an adaptive manner.

The BusterNet method [14] can be considered as the first method that discriminate the original region from the forged one. it introduces a deep neural architecture for image copy-move forgery detection. It employs an end-to-end trainable method, which discriminates the original and forgery region besides detecting similar areas. This network has two branches, and both branches are composed and identified the masks of the original and forgery region (Fig 2).

The purpose of the Mani_Det branch is to detect manipulated areas. As mentioned earlier, in copy-move forgery, original and copied regions are from the same image, and some image features such as color, texture, and noise are the same in both regions. Therefore, detecting the manipulated areas in this branch is very challenging.

The purpose of the Simi_Det branch is to identify similar areas. To achieve this goal, four networks within this branch have been used. The first network extracts feature from the

image. The second network calculates the degree of similarity between the features obtained from the first network. As it has been mentioned, one of the challenges of traditional methods is the high computational complexity in finding the similar features. The third network acquires matching features. Finally, the last network is to restore the original resolution of the image. In traditional methods of detecting copy-move forgery after the matching step a filter is used to remove false similarities. The Simi_Det branch has no plan for the filtering stage, which causes incorrect areas to be matched in smooth areas.

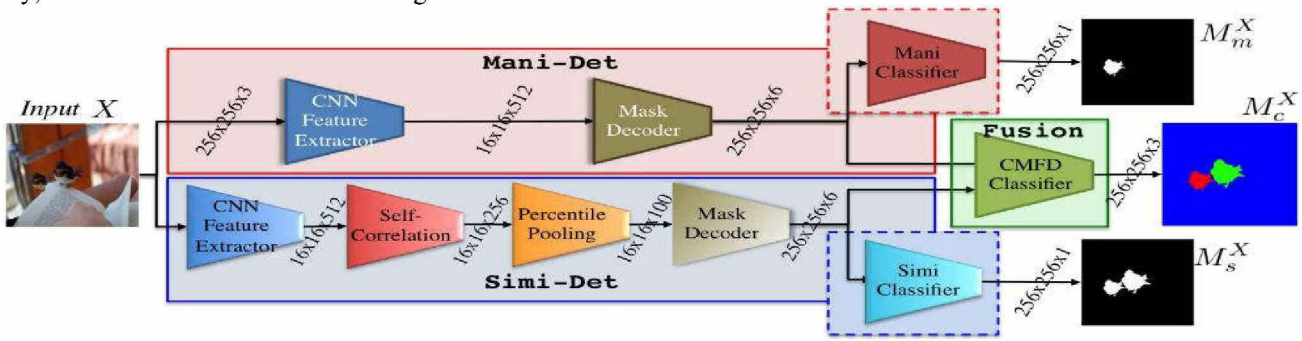

FIG 2. THE BUSRETNET METHOD FRAMEWORK [14]

As mentioned, methods for detecting copy-move, and splicing forgery are different. In copy-move forgery, original and copied regions are from the same image, and some image features such as color, texture, and noise are the same in both regions. As a result, methods for detecting splicing forgery cannot be used to detect copy-move forgery. The result of the copy-move detection is mostly a binary mask in which the tampered regions are not discriminated from the original one. The similarity of the image structure in these two regions makes this discrimination too challenging. Resolving this challenge is our goal in this paper.

III. SEPARATION OF THE FORGED REGION

Many techniques have been proposed to address the challenges of copy-move forgery detection. Most of the previous methods only identify similar patches (original and copied). They are usually based on finding similarity in an image. Finally, they present a binary mask as output (like fig. 3). The mask does not determine which region is the original one. Identification and separating the original region among detected regions due to features similarity is a complicated task which is investigated in this paper.

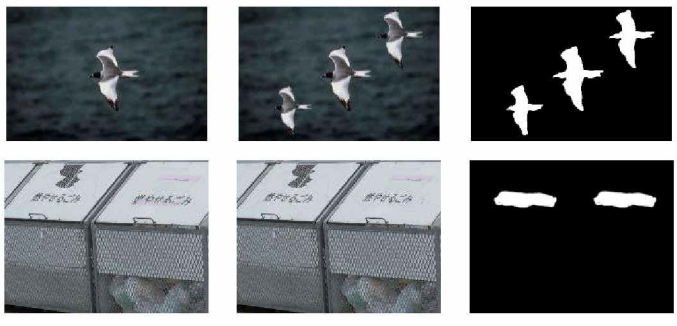

FIG 3. A) ORIGINAL IMAGE B) FORGED IMAGE C) BINARY MASK

In copy-move forgery, forgers usually manipulate the boundaries of the copied snippets to conceal their footprint. This intervention may lead to texture inconsistency. When these changes are performed skillfully, they will be too hard to be recognized by the HVS. Therefore, it can be helpful to examine the inconsistencies in the forged regions. It should be noted that natural images are intrinsically self-similar. Therefore, it can assist a forger to conceal their footprint even without any modification. It makes it too challenging to distinguish between intact and duplicated patches.

The image texture describes the local arrangement of color and intensities. Local texture consistency might be damaged after any manipulation performed to mask the trace of forgeries. As a result, texture analysis can be exploited to discover local inconsistency. Local binary patterns (LBP) [15] is a kind of visual descriptor and one of texture analysis methods which generates proper features for texture classification. Since LBP extracts statistical and structural features of the textures, they are considered as a powerful tool for texture analysis. They are used in many applications such as image quality assessment, face recognition, motion analysis, video and image retrieval, and so on.

When describing an image with LBP, a value will be assigned to each pixel in the image. For computing the LBP value for a pixel, the difference of its intensity with the intensity of its neighbors will be computed. Arbitrary number of neighbor pixels can be considered at an arbitrary radius with respect to the pixel. When considering P neighbor pixels, the binary code for the center pixel will have P digits; one bit for each neighbor pixel. This bit is one, if the value of the neighbor pixel is larger than the center pixel, and will be zero otherwise. This way, a binary number with P digits will be obtained for the center pixel. This binary number is converted to a decimal number which is the LBP value of the pixel. equation(1) [16] formalizes the definition of LBP for a pixel at position (u, v) with P neighbors at radius R.

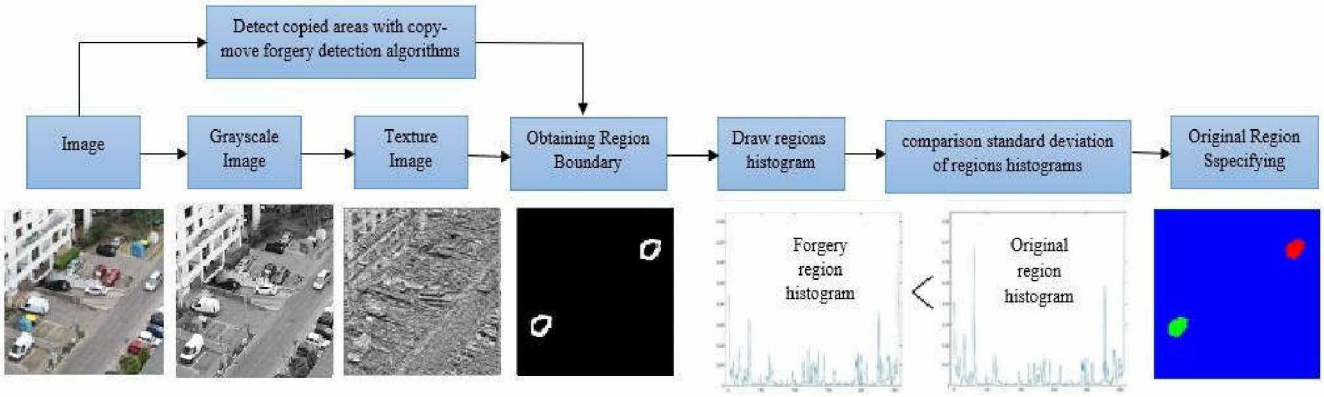

FIG 4. THE PROPOSED METHOD FRAMEWORK

$$LBP_{P,R}(u,v) = \sum_{P=0}^{P-1} I(g_P - g(u,v))2^P \qquad (1)$$

In equation(1) g(u; v) is the intensity of the central pixel in position (u; v). g_p, is the intensity of its neighbors, and I is calculated using (2):

$$I(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \qquad (2)$$

In order to discriminate the forged patches, LBP is applied to the grayscale image. As mentioned, the forger usually manipulates the boundaries of the forged region to eliminate the effect of tampering. Therefore, the histograms of the boundary texture of detected regions are investigated. The histogram is obtained by using (3) [16]:

$$hist(k) = \sum_{i}^{M}\sum_{j}^{N} f(LBP(i.j),k) \quad k \in [0,K] \qquad (3)$$

Where k is the maximum LBP pattern value. M, N are related to *the region under investigation* and the function f shows the frequency each of the image texture values (4).

$$f(x,y) = \begin{cases} 1 & x = y \\ 0 & other\ wise \end{cases} \qquad (4)$$

Since the forged regions are usually modified by a low pass filter in order to disappear its borders with the background, it is expected that the LBP histogram of the duplicated regions will be more smooth. To check the histogram fluctuations, we employ the standard deviation as illustrated in equation (5):

$$s = \left(\frac{1}{n-1}\sum_{i=1}^{n}(hist(i) - \overline{hist})^2\right)^{1/2} \qquad (5)$$

$$\overline{hist} = \frac{1}{n}\sum_{i=1}^{n} hist(i) \qquad (6)$$

Where n is the number of elements of the histogram.

Thus, by calculating the standard deviation of the LBP histogram, it is possible to detect the copied patches. In other words, the standard deviation of the LBP histogram is expected to be less than its counterpart in original snippet. The LBP histogram of a boundary of a forged and an original region is compared in fig.5. (Fig 4. The proposed method framework)

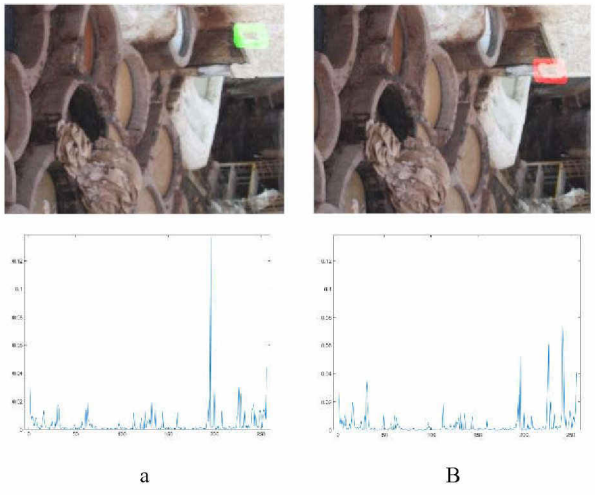

FIG 5. HISTOGRAM BORDERS THE ORIGINAL AND FORGERY REGION IN THE TEXTURE IMAGE A) ABOVE ARE THE BORDERS OF THE ORIGINAL REGION SHOWN IN GREEN AND IS DRAWN AT THE BOTTOM OF THE HISTOGRAM. B) ABOVE ARE THE BORDERS OF THE FORGERY SHOWN IN RED. IT IS DRAWN AT THE BOTTOM OF THE HISTOGRAM.

IV. EXPERIMENTAL RESULTS

In order to evaluate the performance of the proposed method and compare it with the BusterNet method, several experiments have been performed on different datasets.

A. *Dataset*

The CASIAV2 dataset [17] is one of image forgery dataset. This dataset contains 7200 original images and 5123 manipulated images. There are 1313 copy-move forged images. The size of the images in this dataset is from 320×240 to 800 × 600. Before pasting, the forged region is subjected to some kinds of manipulations such as rotation, scale or other damage. After pasting the forgery region, post-processing such as blurring is applied to the border of the forgery region or anywhere else in the image.

The CoMoFoD dataset [18] contains 200 images. The images size is 512 × 512. These images are subjected to five kinds of attacks such as translation, rotation, scaling, distortion and combination.

The GRIP dataset is presented by Cozzolino et al. [13]. This dataset contains 80 images at 1024 × 768, and the copied region have different shapes and sizes. The size of duplicated area size of this dataset is approximately 4,000 (less than 1 percent of the whole image) to 5000 pixels.

B. *Performance evaluation*

LBP uses different radiuses to select neighborhoods. Since the forger usually conceals the trace by using filters which are proportional to image resolution and forged area; we considered a range corresponding to the above mentioned points for the sake of texture analysis . This range of radius is adopted from [18], which is used to investigate the image quality and provides an appropriate scale, based on the resolution of the image. It is needless to say that the forgers should be considered the characteristic of HVS in order to forge an image in a believable manner. According to this range, three different radiuses are considered for LBP. The results are obtained based on these three radiuses. In general, if texture inconsistency is detected in two of the three radiuses , it can be concluded that the region is forged. In our implementation, the number of neighbors is considered as 8 (P = 8) in LBP.

Two methods are used to find the boundaries of the original and forgery region. In the first method, the ground truth which is available in the dataset is used. In the second method, the mask detected by the copy-move forgery algorithms is used. The reason for using copy-move forgery algorithms at this stage is the lack of proper ground truth in practical terms. In this research, the PatchMatch method [13], which is one of the most popular methods in the field of copy-move forgery, is used to identify similar region and their borders.

In some datasets, multiple copy-move forgeries occur in a single image. Therefore, the results will be presented in the proposed method based on the number of similar patches.

Since copy-move forgery detection methods sometimes do not identify masks in the original and forged region, so some images cannot be used to test the method. Also, in the BusterNet method, in all cases, it cannot identify the two original and forgery regions. Therefore, the proposed method and the BusterNet method have been evaluated by two accuracy measurements. Overall accuracy shows the ratio of correctly detected samples to the total sample. *Opt_in* accuracy indicates the ratio of correctly detected samples to the number of *Opt_in* batch images.

TABLE1: COMPARISON OF PROPOSED METHOD AND BUSTERNET METHOD 1 IN DATASET CASIA

		Number of Images			Accuracy	
		Total	Opt_in	Correct	Opt_in	Overall
Proposed feature	Ground truth	1333	---	875	---	65.64
	Detected Mask	1333	488	221	45.29	16.58
BusterNet		1311	580	133	66.9	6.8

TABLE 2: COMPARISON OF PROPOSED METHOD AND BUSTERNET METHOD 1 IN DATASET COMOFOD

		Number of Images			Accuracy	
		Total	Opt_in	Correct	Opt_in	Overall
Proposed feature	Ground truth	214	---	103	---	48.13
	Detected Mask	214	94	47	50	21.96
BusterNet		200	33	23	69.7	11.5

TABLE 3: COMPARISON OF PROPOSED METHOD AND BUSTERNET METHOD 1 IN DATASET GRIP

		Number of Images			Accuracy	
		Total	Opt_in	Correct	Opt_in	Overall
Proposed feature	Ground truth	80	---	54	---	67.5
	Detected Mask	80	79	53	67.09	66.25
BusterNet		80	3	0	0	0

Tables 1, 2 and 3 show the results on the Casia, CoMoFoD and GRIP datasets respectively. As you can see in the tables, the proposed method discriminates the original region from the forgery one more accurately than BusterNet method. Since it is supposed that the forger has manipulated the boundaries of the forgery region, the proposed method works better where it is needed to hide the forgery. But sometimes due to the self-similarity in the image and where

the areas are highly textured, the forger can easily hide the forgery without the need for manipulation, and the proposed method does not work well in these images. Therefore, in the CoMoFoD dataset, the detection percentage in the proposed method is lower because the forged regions have a high self-similarity.

V. CONCLUSION

Copy-move forgery detection methods are mostly based on finding similar regions. They provide a binary mask as their output, in which each pixel is identified as either background or copy-move pixels. In this paper, a method for discriminating the duplicated region from the original one is presented. Our method employs texture information of the border regions of detected copy-move regions. Since the original and forged region are parts of the same image, detecting the duplicated snippet is a challenging task.

REFERENCES

[1] Boididou, C., et al., *Verifying information with multimedia content on twitter.* Multimedia Tools and Applications, 2018. **77**(12): p. 15545-15571.

[2] Pun, C.-M., B. Liu, and X.-C. Yuan, *Multi-scale noise estimation for image splicing forgery detection.* Journal of visual communication and image representation, 2016. **38**: p. 195-206.

[3] Bahrami, K. and A.C. Kot. *Image tampering detection by exposing blur type inconsistency.* in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2014. IEEE.

[4] Zandi, M., A. Mahmoudi-Aznaveh, and A. Talebpour, *Iterative copy-move forgery detection based on a new interest point detector.* IEEE Transactions on Information Forensics and Security, 2016. **11**(11): p. 2499-2512.

[5] Fridrich, A.J., B.D. Soukal, and A.J. Lukáš. *Detection of copy-move forgery in digital images.* in *in Proceedings of Digital Forensic Research Workshop*. 2003. Citeseer.

[6] Li, Y., *Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching.* Forensic science international, 2013. **224**(1-3): p. 59-67.

[7] Ryu, S.-J., et al., *Rotation invariant localization of duplicated image regions based on Zernike moments.* IEEE Transactions on Information Forensics and Security, 2013. **8**(8): p. 1355-1370.

[8] Huang, H., W. Guo, and Y. Zhang. *Detection of copy-move forgery in digital images using SIFT algorithm.* in *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*. 2008. IEEE.

[9] Amerini, I., et al. *Geometric tampering estimation by means of a SIFT-based forensic analysis.* in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. 2010. IEEE.

[10] Li, J., et al., *Segmentation-based image copy-move forgery detection scheme.* IEEE Transactions on Information Forensics and Security, 2014. **10**(3): p. 507-518.

[11] Lin, C., et al., *Region duplication detection based on image segmentation and keypoint contexts.* Multimedia Tools and Applications, 2018. **77**(11): p. 14241-14258.

[12] Barnes, C., et al. *PatchMatch: A randomized correspondence algorithm for structural image editing.* in *ACM Transactions on Graphics (ToG)*. 2009. ACM.

[13] Cozzolino, D., G. Poggi, and L. Verdoliva, *Efficient dense-field copy–move forgery detection.* IEEE Transactions on Information Forensics and Security, 2015. **10**(11): p. 2284-2297.

[14] Wu, Y., W. Abd-Almageed, and P. Natarajan. *BusterNet: Detecting copy-move image forgery with source/target localization.* in *Proceedings of the European Conference on Computer Vision (ECCV)*. 2018.

[15] Ojala, T., M. Pietikäinen, and D. Harwood, *A comparative study of texture measures with classification based on featured distributions.* Pattern recognition, 1996. **29**(1): p. 51-59.

[16] Muthevi, A. and R.B. Uppu. *Leaf classification using completed local binary pattern of textures.* in *2017 IEEE 7th International Advance Computing Conference (IACC)*. 2017. IEEE.

[17] Dong, J., W. Wang, and T. Tan. *Casia image tampering detection evaluation database.* in *2013 IEEE China Summit and International Conference on Signal and Information Processing*. 2013. IEEE.

[18] Tralic, D., et al. *CoMoFoD—New database for copy-move forgery detection.* in *Proceedings ELMAR-2013*. 2013. IEEE.

[19] Daoud, A.O., A.A. Tsehayae, and A.R. Fayek, *A guided evaluation of the impact of research and development partnerships on university, industry, and government.* Canadian Journal of Civil Engineering, 2017. **44**(4): p. 253-263.