Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 61 – 67

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques

Anil Dada Warbhe[a*], R. V. Dharaskar[b], V. M. Thakare[c]

[a]*Research Scholar, SGBAU, Amravati 444602, India*
[b]*Former Director, DES (Disha–DIMAT) Group of Institutes, Raipur 492101, India*
[c]*HOD, SBGAU (PG Dept. of Computer Science), Amravati 444602, India*

Abstract

Copy-Move forgery is the most common image tampering method to create forged images. The images may be forged to conceal or change the meaning of the photographs. Hence, it becomes important to verify the integrity and authenticity of the images. The copy-move forgery detection can be classified under two heads viz., block based and keypoint based. The block based methods use mostly the similar kind of frameworks but differ in applying feature extraction schemes. The block-based methods are good at detecting the forged regions with high accuracy but is having tremendously high computational complexity. In this paper we review the keypoint approach which is an alternative to block-based approach. The keypoint based copy-move forgery detection schemes involve, detecting and describing the local features of the images by using the algorithms like SIFT and SURF.

Peer-review under responsibility of organizing committee of the ICISP2015

*Keywords:*Digital Image forensics; Image Forgery; Image Tampering; Copy-Paste Forgery.

1. Introduction

Copy-move forgery is a type of image forgery in which a portion of the digital image is copied from one place and pasted somewhere in the same image. Fig. 1 shows one such example. In the literature, we can find some forgery detection techniques[34-36] proposed, to detect and locate the forgery that can be classifiedunder different

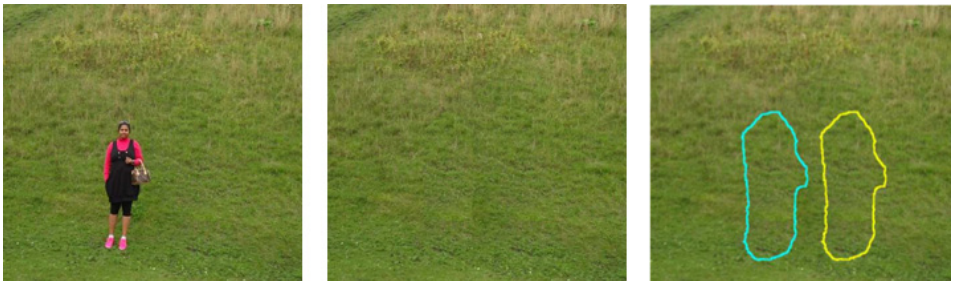
* Corresponding author. Tel.: +91-982-355-1869.
*E-mail address:*mtech2008@rediffmail.com

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.011

heads. Broadly, these techniques are based on two approaches. The first one is the block based approach; that divides the digital image into the number of blocks and extract the features from it. The other one is a keypoint based forgery detection, which rely on the identification and selection of high-entropy image regions.

In block based survey[1], it has been observed that; most of these techniques are good for accurate detection and location of the copy-move forgeries. However, the main concern with these techniques is their computational intensiveness. Also, most of the block-based techniques fails when the copied portion of an image goes through some operation such as scaling, rotation,etc. To answer this, researchers come up with another approach known as keypoint based approach. Keypoint based techniques base on identifying and selecting high-entropy image regions. Here, the feature vector is extracted per keypoint. Consequently, fewer feature vectors are estimated, resulting in reduced computational complexity of feature matching and post-processing. The lower number of feature vectors indicates that post-processing thresholds are also to be lower than that of block-based methods[2].

In this paper, we present a state of the art on keypoint based copy-move forgery detection. Block-based techniques mainly use the algorithms, such as Principle Component Analysis (PCA), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD),etc. Whereas, keypoint based approach mainly uses the scale and rotation-invariant interest point/feature detector and descriptor algorithms. Two such algorithms are Scale Invariant Feature Transform (SIFT) and Speeded-up Robust Features (SURF).



(a) (b) (c)

Fig. 1. Copy paste forgery and it's detection (a) Original image; (b) Forged Image; (c) Forgery detection results. [37]

2. Local Feature Detector and Descriptors

The keypoint based algorithms in the literature usually require two steps for detecting and describing local visual features. In the first step, the localization of the interest point is done. In the second step, the construction of the robust local descriptors is done, such that it should be invariant to affine transformations. The local visual features have been widely used for image retrieval and object recognition, due to its robustness to several geometrical transformations such as rotation, scaling, occlusions and clutter [3]. In the literature, keypoint based copy-move forgery detection is mostly based on SIFT and SURF. Both of them are image local feature description algorithms based on scale-space. In this paper, we review the methods based on these techniques.

2.1. Scale Invariant Feature Transform (SIFT):

Scale Invariant Feature Transform was developed by David Lowe in 2004 as a continuation of his previous work on invariant feature detection (Lowe, 1999). The author proposed a method for detecting distinctive invariant features from images that can be later used to perform reliable matching between different views of an object or scene. The main key concepts used here are: first is the distinctive invariant features and second is reliable matching.

The features detected by SIFT are more suited for reliable matching in the images, as it uses the cascade filtering approach to detect the features that transform image data into scale-invariant coordinates relative to local features. It is comprised of four main steps[4] 1) Scale-Space extrema detection; 2) Keypoint localization and filtering; 3) Orientation assignment; and 4) Keypoint descriptors.

The first two steps are the detector and later two are known as descriptor stages. At each stage, a filtering process is incorporated so as to pass on only key points that are robust enough. The whole SIFT algorithm can be briefed as, for an image *I*, SIFT returns a list of *N* keypoints, each of which is completely described by the information: $X_i=\{x, y, \sigma, o, f\}$. Where, (x, y) are the coordinates in the image plane; σ is the scale of the keypoint;*o* is the canonical orientation, which is used to achieve geometric transformation invariance, and *f* is the final SIFT descriptor.[3]

2.2. Speeded Up Robust Features (SURF):

The Speed Up Robust Feature detector (SURF) was proposed by Bay et al. 2006 [5] and ensures the high speed in three of the feature detection steps: detection,description, and matching. Due to theuse of the Hessian matrix's trace, the matching speed has been significantly improved over the SIFT. The SURF algorithm speeds up the SIFT's detection process without scarifying the quality of the detected points. Here the scale-space is created by selecting the different size box filter convolved with the integral image. The potential keypointsare detected by using the Hessian matrix and Non-maximum suppression. For the assignment of one or more canonical orientations, a sliding orientation window of size *pi/3* detects the dominant orientation of the Gaussian weighted Harr wavelet responses at every sample point within a circular neighborhood around the interest point. The descriptor consists of an oriented quadratic grid with 4×4 square sub-regions. Itis laid over the interest point, and for each square the wavelet responses are computed from 5×5 samples. For each field the sums of dx, $|dx|$, dy, $|dy|$ are collected and computed relatively to the orientation of the grid.

3. Methods Based on Scale Invariant Feature Transform

In the following section, we review the copy-move forgery detection techniques using SIFT.

Huang et al. [6] used SIFT for computing local statistical features of an image. The proposed algorithm uses the best-bin-first nearest-neighbor for matching keypoints. It is rotation and scale invariant but lacks in performance.

Zhang et al. [7] proposed a novel approach. It consists of three steps. In thefirststep, they have used modified ESS (Efficient Subwindow Search algorithm) twice to detect and locate the duplicated region pairs. In step two they have used planar homography constraint to segment, duplicate regions, and in third step they differentiate the authentic region from the tampered one by analyzing their contours. The experimental results show the robustness of the algorithm with geometric manipulation and background clutter.

The proposed algorithm[8] involves three steps: keypoint clustering, cluster matching, and texture analysis. For clustering the keypoints, the hierarchical tree clustering algorithm is used. The algorithm does texture based analysis to find the similar cluster matching. The algorithm is Robust to false matches and gives good results unto JPEG compression level of 30. The drawback is, algorithm fails if the number of clusters formed is too small or very large.

Amerini et al.[3,9] proposed three step method. The first is SIFT feature extraction and similar feature matching. To find the similar keypoints iterative generalized 2NN test is used. The second step uses agglomerative hierarchical clustering to form the clusters of the features. Geometric Transformation is estimated in the third step. The method can detect multiple cloned regions. But, the algorithm fails to localize the tampering accurately, and it cannot detect the copied image patch having maximum uniform texture such as the salient keypoints that are not covered by SIFT.

In the algorithm proposed by Pan and Lyu[10], SIFT is used to find image keypoints and then image features are collected at those keypoints. The detected keypoints are matched based on their feature vectors. The Best-bin-First algorithm is used for matching the keypoints. The geometric distortions of the pasted regions are estimated using random sample consensus (RANSAC). The algorithm is found to be robust against additive noise, geometric transformation, and JPEG image compression. The accuracy rate is high as it detects the duplicate regions precisely.

Shivakumar and Baboo[11] use Harris detector to detect keypoints, which is faster than SIFT. SIFT is used to generate feature descriptor of the extracted keypoints. The kd-tree algorithm is used to match keypoints and to detect matched duplicated regions. The algorithm is robust to Gaussian noise, scaling, and rotation.

Authors in[12] use SIFT and DWT. The DWT is used for dimensionality reduction. DWT is carried outof an image to decompose it into four parts LL, LH, HL, and HH. Assuming the only LL part of the image contains most of the information, the SIFT features are extracted from the LL part. This extracts the key features and find descriptor vector of these key features and then find similarities between various descriptor vectors. The main advantage of this

proposed method is its high accuracy as compared to other methods and reduced computation complexity. As it first divides the image into the four parts, the efficiency of the algorithm is affected by the image size.

Liu, Bo, and Chi-Man Pun proposed a method[13] in which, the SIFT features are first compared to pair analogous feature points. As, once these matched interest points are paired and the keypoints are localized it is important to remove falsely matched points, if any, in the second step. They are removed by applying the distance examination. The second step is important in the sense that it improves efficiency and reduces computational complexity. In the third stage, the block color feature inspection is done. Normalized RGB color feature of matched point's neighborhood is extracted, and the output of neighboring keypoint removing step is inspected. The color difference of each pair is recorded to calculate the median value of differences, so as to detect and eliminate the outliers. Finally, a block texture feature is applied to discard the remnant false matched pairs from the previous steps. The algorithm effectively detects altered regions even after the changes in the geometry and shading of the copied area.

The authors' in[14] proposed a novel method to detect the combination of different post-processing operations. The method uses the combination of DCT and SIFT. As DCT is robust against the JPEG compression and the Gaussian noise due to strong energy and SIFT is robust against the rotation and scaling. Hence, the proposed method is able to detect the forgery in the images even it has gone under different post-processing operations. The forgery detection rate is increased as if one method fails to detect the forgery the other succeeds in detecting the forgery.

The proposed method[15]is improved version of the earlier[3] proposed algorithm. Here the clustering object became a vector associated with the candidate transform estimation. A better estimation of the cloned area is very important in order to obtain an accurate forgery localization. The forged images, in which the copied portion contains pixels that are spatially very distant among them, and when the pasted area is near to the source, it becomes very difficult to locate the forged regions. To address this issue, the authors presents a novel approach based on an adaptation of the J-Linkage algorithm. The algorithm consists of three steps: In the first step of the algorithm the extraction of SIFT feature and keypoint matching is done, in the second step clustering and forgery detection is done, while in the third step the localization of the copied region, if a tampering has been detected, is done.

The authors' proposed[16] an improved SIFT based algorithm. The local interest points are detected, and the SIFT features for such keypoints are computed. At each interest point, a 128-dimensional feature vector is generated from the histogram of local gradients in its neighborhoods. After this, feature matching based clustering is performed on coordinates of the matched points. After clustering, keypoint matching is done. It mainly concerns with the matching of extracted feature keypoints from SIFT algorithm. Finally, the algorithm determines which geometrical transformation was used on the original portion of the image. For this, Homographic matrix of at least three matched points is computed. This 3x3 matrix is computed using maximum likelihood estimation of the homography.

The paper[17] uses a combination of color Coherence Vector (CCV) and SIFT. CCV is used to determine the similarity in an image. The number of coherent versus incoherent pixels with each color is stored by separating coherent pixels from incoherent pixels using CCV. The vector will designate the coherence of the colors in a region. It uses block-basedapproach but assumes that the forged regions might have gone through the rotation. The SIFT is used to calculate the match points and show matching points by first rotating the image by some angle.

Jeberi et al. proposed[18] a SIFT based algorithm which is Mirror reflection Invariant. The authors named it MIFT (Mirror reflection Invariant Feature Transform). The features extracted by MIFT are invariant to affine transform as that to SIFT but in addition to that, MIFT features are reflection invariant. First, from the image, they find corresponding features using SIFT matching. In the second step affine transformation between similar regions is estimated using RANSAC. In the third step, the affine transformation parameters are refined iteratively, by slowly increasing the search window around the corresponding regions. The objective of this step is to refine the affine transformation parameters estimated from the previous step. Finally, the actually forged regions are localized.

The proposed approach[19] combines sift with broad first Search neighbors (BFSN) clustering and color filter array (CFA) features. Authors' use SIFT to extract distinctive local features in the image. The clustering of the keypoints are done using BFSN clustering algorithm, and the clusters are then matched to solve the problem of multiple copies detection. The specific correlations between adjacent pixels arebeing introduced for CFA interpolated images. When copy-move forgery occurs,its likely to be destroyed. Hence, CFA features are used to distinguish the original regions from the tampered regions by detecting the inconsistency among the adjacent pixels. The main advantage of the proposed algorithm is that it can detect multiple copied regions and discriminates original and forged regions.

Takwa Chihaoui et al. proposed[20] a hybrid method based on SIFT and SVD. In this algorithm, the forgery detection is done by identifying the keypoints of an image using SIFT and matching identical features using SVD. Firstly, the image undergoes the SIFT transform and calculates the locations of interest point invariant to scale and orientation. In thesecond step, features are extracted from detected keypointsin order to eliminate more keypoints from the list by finding those that are likely to remain stable over transformations. The third stage identifies the dominant orientations for each selected key-point based on its local image patch. In the final stage, a local feature descriptor is computed at each keypoint based on a patch of pixels in its local neighborhood. So, the output of this step is SIFT keypoints that are represented with 128-dimensional descriptor vectors and their locations. The proposed method reduces the number of falsepoints matching problem and is robust to geometrical transformations.

The proposed method[21] uses acombination of both keypoint and block based approach. The authors propose an adaptive over-segmentation algorithm, which segments the suspicious image into irregular and non-overlapping blocks adaptively. After that, keypoints are extracted from each block using SIFT as block features. These block features are matched to locate the labeled feature points. This approximately detects the suspected forged regions. However, to detect exact forged regions authors has proposed Forgery Region Extraction Algorithm (FREA). The FREA replaces the feature points with small super pixels as feature blocks. These feature blocks are then merged with the neighboring blocks having the similar local color features into the feature blocks to generate the merged regions. At last, themorphological operation is applied to the merged regions to detect the forged regions accurately.

The authors[22] proposes an algorithm which significantly raise the accuracy of localization of copy-move forged regions. SIFT is used to get the keypoints, and they are clustered using k-means algorithm. The contrast context histogram (CCH) features are used to detect the copy-move forgery effectively. The localization of these forged regions is done using disparity map. The disparity map is created using thesum of absolute difference of the keypoints to localize these regions. Similarly, Shen et al.[33] used the combination of SIFT and HIS; the algorithm is not only robust to the JPEG compression, white noise, and Gaussian blur but also reduces the false matching rate.

4. Methods Based on Speeded up Robust Features

In this section, we review the forgery detection methods based on SURF and combination of SURF and SIFT.

Bo, Junwen, Guangjie and Yuewei, proposed[23] a SURF based algorithm. It uses Hessian matrix for detecting the keypoints and Haar wavelets for assigning the orientation. The dominant orientation is estimated, and the orientation of the interest point descriptor is described. The square regions are extractedaround these interest points, and then SURF descriptors are constructed, which are aligned to the dominant orientation. The authors have chosen Haar wavelets because they are invariant to the illumination bias;it is also useful in increasing the robustness to localization errors and geometric deformations. The SURF descriptors are then used for matching. The algorithm is found to be robust for these post processing operations like blurring, scaling, and rotation and the forged regions are accurately detected. The algorithm, however, failed to detect the exact boundaries of the tampered region.

Shivakumar and Baboo proposed an algorithm[24] in which, they have first extracted the SURF features. In the second step,key-point matching is done. After that, a verification step is performed which filters matching pairs that follow a common pattern. The experiments carried out show that the algorithm detects copy-move forgery with a minimum false positive. The algorithm is even robust to rotation, scaling, and Gaussian noise.

Guang-qun Zhang and Hang-jun Wang proposed[25] an algorithm to detect forgeries in flat and non-flat regions. Assuming the test image consisting of both flat and non-flat region the proposed method first separates these two regions. The forged regions are detected by both block based and keypoint approach. For forgery detection in thenon-flat region first the keypoints are detected using SURF. In second step feature pruning and matching is done. Finally, the region transform is estimated, and duplicated regions are identified using correlations adjusted with the estimated transforms. For the forgery detection in flat regions, authors have proposed a different method. In the first step, the flag image regions are detected. The main purpose of flat region detection here is to locate the regions that keypoint matching based methods fails. In the next step, image blocking in flat regions and Fourier-Mellin Transform (FMT) feature extraction of the image block is performed. Finally, duplicate regions are identified.

Mishra et al. proposed[26] algorithm based on SURF and agglomerative hierarchical clustering (AHC). Keypoint detection and feature extraction of the test image is done using SURF. After that, two different keypoints are chosen then sort the inverse cosine angles of the dot products between each keypoint feature descriptor with the others.

Now, if the ratio of two nearest neighbors is less than 0.6 then it is confirmed that the match exists, and the coordinates are stored else the same procedure after choosing the two keypoints is repeated. Algorithm now checks if all keypointsare processed if not then theprocess has to be repeated by taking two keypoints again otherwise AHC is performed on the matched key points to obtain copy-move forgery detection.

Mohammad Hashmi et al.[27] proposed combining SURF and Wavelet Transform. The imageis first transformed into wavelet domain. SURF is applied on this transformed image for keypoints detection and feature extraction. The SURF feature descriptor vector is obtained. Because of the multispectral components produced by the wavelet, the features are more predominant. The algorithm finds amatch between the descriptor vectors and marks forged regions.

Authors proposed[28,29] a fast and robust copy-move forgery detection using the combination of SURF and SIFT image features. The proposed method is a two stage process. In the first stage, both SIFT and SURF keypoints are detected, and feature descriptors are computed. Then generalized 2-nearest neighbors (g2NN) is applied which after dynamic thresholding detects the forged regions from the suspected image. Fusing two feature detection method increases the efficiency and robustness of forgery detection but at the same time number of keypoints affect processing time and also cannot detect multiple cloned regions with highly uniform texture.

Salma Amtullah and Ajay Koul has proposed a method[30] based on SURF. The features of the test image are extracted, and their descriptors are obtained. The Nearest Neighbour approach is used for feature matching and thereby for identifying the copy-move forgery. The method is rotation and scale invariant and is robust to noise, jpeg compression, and blurring. The proposed method can be used for detecting multiple copy-moveforgeries.

The authors have proposed a novel approach[31] based on voting processes and multi-scale analysis of a suspicious digital image. The keypoints are extracted using SURF. The corresponding points are clustered into the regions based on geometric constraints. After that, a multi-scale image representation is constructed using a descriptor strongly robust to the affine transform and partially robust to compression.For each scale, the generated groups are examined. This decreases the search space of duplicated regions and yields a detection map. A voting process among all detection maps is carried out to identify and locate forgeries in the image.

Authors have proposed a hybrid approach[32]. Two different methods are used for keypoint detection and description. The keypoints are detected by SURF, and then extract Binary Robust Invariant Scalable Keypoints (BRISK) features at these keypoints. These binary features from BRISK are matched for similarity using knn search. Hamming distance is used to find thenearest neighbor. The distance ratio of the two instant neighbors of a point is compared with a threshold value ranges from 0.3 to 0.5, to discard the outliers. The Proposed method is robust to affine transform and to the post-processing operations such as adding JPEG compression and Gaussian noise.

5. Conclusion

The main drawback of block-based approaches detecting copy-move forgery is the high computation time. In block-based approach, the image needs to be divided into the number of blocks and each block is processed for feature extraction and matching. The image size, block size, and offset chosen for dividing an image affects the forgery detection significantly. As compared to the block-based approach, keypoint based approach excels not only in computation time but memory consumption as well. Their feature size is relatively large, but the extracted keypoints are typically far smaller in magnitude than that of the image blocks. The keypoint based approach is found to be robust against the post processing operations such as scaling, rotation, JPEG compression, Gaussian noise, and illumination in which block based approach fails. Though block based approach is good in detecting the exact forgery region, keypoint based approach excels in all other aspects as discussed above. Hence, keypoint based approach becomes the ideal choice for copy-paste forgery detection in large size images over block based approach.

References

1. Warbhe A, Dharaskar R, Thakare V. Block Based Image Forgery Detection Techniques. Int J Eng Sci Res Technol. 2015;4(8):289–97.
2. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copy-move forgery detection approaches. Inf Forensics Secur IEEE Trans On. 2012;7(6):1841–54.
3. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G. A sift-based forensic method for copy–move attack detection and transformation recovery. Inf Forensics Secur IEEE Trans On. 2011;6(3):1099–110.

4. Lowe DG. Distinctive image features from scale-invariant keypoints. Int J Comput Vis. 2004;60(2):91–110.
5. Bay H, Ess A, Tuytelaars T, Van Gool L. Speeded-up robust features (SURF). Comput Vis Image Underst. 2008;110(3):346–59.
6. Huang H, Guo W, Zhang Y. Detection of copy-move forgery in digital images using SIFT algorithm. In: Computational Intelligence and Industrial Application, 2008 PACIIA'08 Pacific-Asia Workshop on. IEEE; 2008. p. 272–6.
7. Zhang C, Guo X, Cao X. Duplication localization and segmentation. In: Advances in Multimedia Information Processing-PCM 2010. Springer; 2010. p. 578–89.
8. Ardizzone E, Bruno A, Mazzola G. Detecting multiple copies in tampered images. In: Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE; 2010. p. 2117–20.
9. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G. Geometric tampering estimation by means of a SIFT-based forensic analysis. In: Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on. IEEE; 2010. p. 1702–5.
10. Pan X, Lyu S. Region duplication detection using image feature matching. Inf Forensics Secur IEEE Trans On. 2010;5(4):857–67.
11. Shivakumar B, Baboo SS. Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors. Int J Comput Appl. 2011;27(3):9–17.
12. Hashmi MF, Hambarde AR, Keskar AG. Copy move forgery detection using DWT and SIFT features. In: Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on. IEEE; 2013. p. 188–93.
13. Liu B, Pun C-M. A SIFT and local features based integrated method for copy-move attack detection in digital image. In: Information and Automation (ICIA), 2013 IEEE International Conference on. IEEE; 2013. p. 865–9.
14. Kaur A, Sharma R. Copy-move forgery detection using DCT and SIFT. Int J Comput Appl. 2013;70(7):30–4.
15. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Del Tongo L, Serra G. Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process Image Commun. 2013;28(6):659–69.
16. Swapnil HK, Gawande A. Copy-Move Attack Forgery Detection by Using SIFT. Int J Innov Technol Eng IJITEE. 2013;2(5).
17. Bharamagoudar SR, Mudaraddi NV. FORGERY DETECTION IN IMAGE USING CCV AND SIFT. Int J Res Innov Eng Technol. 2014;1(02).
18. Jaberi M, Bebis G, Hussain M, Muhammad G. Accurate and robust localization of duplicated region in copy–move image forgery. Mach Vis Appl. 2014;25(2):451–75.
19. Liu L, Ni R, Zhao Y, Li S. Improved SIFT-Based Copy-Move Detection Using BFSN Clustering and CFA Features. In: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on. IEEE; 2014. p. 626–9.
20. Chihaoui T, Bourouis S, Hamrouni K. Copy-move image forgery detection based on SIFT descriptors and SVD-matching. In: Advanced Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on. IEEE; 2014. p. 125–9.
21. Pun C-M, Yuan X-C, Bi X-L. Image Forgery Detection Using Adaptive Over-Segmentation and Feature Points Matching. 2015;
22. Vaishnavi D, Subashini T. A passive technique for image forgery detection using contrast context histogram features. Int J Electron Secur Digit Forensics. 2015;7(3):278–89.
23. Bo X, Junwen W, Guangjie L, Yuewei D. Image copy-move forgery detection based on SURF. In: Multimedia Information Networking and Security (MINES), 2010 International Conference on. IEEE; 2010. p. 889–92.
24. Shivakumar B, Baboo LDSS. Detection of region duplication forgery in digital images using SURF. IJCSI Int J Comput Sci Issues. 2011;8(4).
25. Zhang G, Wang H. SURF-based Detection of Copy-Move Forgery in Flat Region. Int J Adv Comput Technol. 2012;4(17).
26. Mishra P, Mishra N, Sharma S, Patel R. Region Duplication Forgery Detection Technique Based on SURF and HAC. Sci World J. 2013;2013.
27. Hashmi MF, Anand V, Keskar AG. A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. In: Computer and Communication Technology (ICCCT), 2014 International Conference on. IEEE; 2014. p. 147–52.
28. Pandey RC, Singh SK, Shukla K, Agrawal R. Fast and robust passive copy-move forgery detection using SURF and SIFT image features. In: Industrial and Information Systems (ICIIS), 2014 9th International Conference on. IEEE; 2014. p. 1–6.
29. Pandey RC, Agrawal R, Singh SK, Shukla K. Passive Copy Move Forgery Detection Using SURF, HOG and SIFT Features. In: Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Springer; 2015. p. 659–66.
30. Amtullah S, Koul A. Passive Image Forensic Method to detect Copy Move Forgery in Digital Images. IOSR J Comput Eng. 2014;16(2):96–104.
31. Silva E, Carvalho T, Ferreira A, Rocha A. Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. J Vis Commun Image Represent. 2015;29:16–32.
32. Kumar S, Desai J, Mukherjee S. A Fast Keypoint Based Hybrid Method for Copy Move Forgery Detection. Int J Com Dig Sys. 2015;4(2).
33. Xuan-jing S, Zhu Y, Ying-da L, Hai-peng C. Coloured image copy-move forgery detection based on SIFT and HSI. J Jilin Univ Technol Ed. 2014;(1):171–6.
34. Zhong J, Gan Y. Detection of copy–move forgery using discrete analytical Fourier–Mellin transform. Nonlinear Dyn. 2015;1–14.
35. Li J, Li X, Yang B, Sun X. Segmentation-based Image Copy-move Forgery Detection Scheme. Inf Forensics Secur IEEE Trans On. 2015;10(3):507–18.
36. Cozzolino D, Poggi G, Verdoliva L. Efficient Dense-Field Copy–Move Forgery Detection. Inf Forensics Secur IEEE Trans On. 2015;10(11):2284–97.
37. Kakar P, Sudha N. Exposing postprocessed copy–paste forgeries through transform-invariant features. Inf Forensics Secur IEEE Trans On. 2012;7(3):1018–28.