COPY - MOVE IMAGE FORGERY DETECTION SYSTEM USING HYBRID METHOD

S. Devi Mahalakshmi (Associate Professor), Department of Computer Science and Engineering
Mepco Schlenk Engineering College, Sivakasi
sdevi@mepcoeng.ac.in

Abstract - **In recent years, digital images are in use in a wide range of applications and for multiple purposes. There are many types of image forgery, the most important and popular type is called copy move forgery, which uses the same image in the process of forgery. The proposed scheme integrates both block-based and keypoint-based forgery detection methods. First, the proposed adaptive over segmentation algorithm segments the input image into non overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labelled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the forgery region extraction algorithm, which replaces the feature points with small superpixels as feature blocks and then merges the neighbouring blocks that have similar local color features into the feature blocks to generate the merged regions. Finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy–move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy–move forgery detection methods.**

Index Terms – **Copy-Move Forgery Detection, SIFT, SLIC, DWT, adaptive over-segmentation, local color feature, forgery region extraction.**

I. INTRODUCTION

In recent years, digital images are in use in a wide range of applications and for multiple purposes. They also play an important role in the storage and transfer of visual information, especially the secret ones. With this widespread usage of digital images, in addition to the increasing number of tools and software of digital images editing, it has become easy to manipulate and change the actual information of the image. Therefore, it has become necessary to check the authenticity and the integrity of the image by using modern and digital techniques, which contribute to analysis and understanding of the images content, and then make sure of their integrity.

The existing system makes use of the several processes. The input images were transformed based on the Discrete Cosine Transformation (DCT) process. The DCT values extracted from the images were reduced based on optimization process based Principal Component Analysis (PCA). Transformations like Discrete wavelet Transform (DWT), Singular Value Decomposition (SVD) and Fourier-Mellin Transform (FMT) were employed for the identification of the copy move regions in the images. The block features were measured based on Zernike moments, Average Gray value and entropy were extracted as block features for the identification of the copy move regions in the images.

The process were based on block matching process and hence when the image size increases the time complexity and algorithm complexity increases and also the features extracted based on the block based approaches. If there are some transformations in the copy move regions the block based methods cannot exactly identify the copy move areas. The shape regions cannot be exactly identified based on the block based approaches. The performance of the process measured based on performance metrics indicates that the approaches needs improvement further.

An optimal solution for this problem is employed based on the feature point based and block based matching process. The block size of the images was calculated based on the input image’s DCT transformation. The images were over segmented with the help of Simple Linear Iterative Clustering (SLIC) algorithm. The SLIC algorithm segments the images based on the block size determined using DCT transformation. SLIC uses the same compactness parameter (chosen by user) for all super pixels in the image. If the image is smooth in certain regions but highly textured in others, SLIC produces smooth regular-sized super pixels in the smooth regions and highly irregular super pixels in the textured regions.

The block features (BF) were extracted based on Scale Invariant Feature Transformation (SIFT) process. For any object in an image, interesting points on the object can be extracted to provide a "feature description" of the object. From the block features extracted labelled feature points (LFP) were calculated. The LFP were matched in order to identify the forged regions in the images. The performance of the process is measured with the help of performance metrics like Precision, Recall value estimated.

II. RELATED WORK

Copy-Move is a specific type of image tampering, where a part of the image is copied and pasted into another part of the same image (Fig 1).

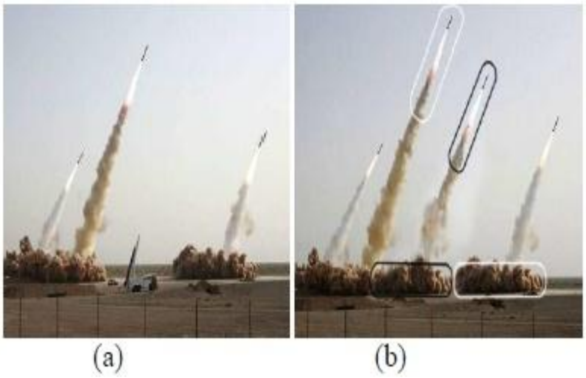


Fig 1: An example of copy-move forgery: (a) three missiles in original image (b) four missiles in tampered image.

In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms [1]–[13] and feature keypoint-based algorithms [14]–[19].

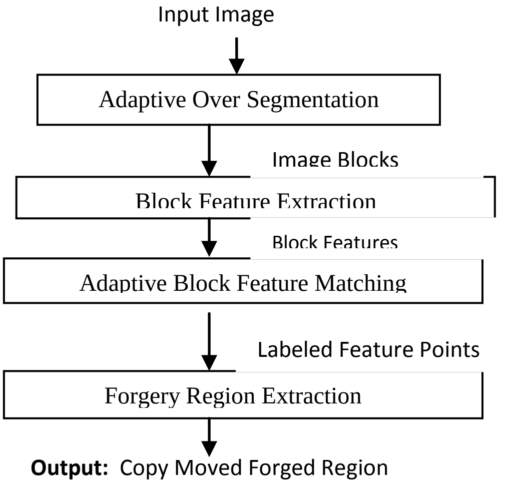
The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Fridrich et al. [1] proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. Popescu and Farid [2] applied Principal Component Analysis (PCA) to reduce the feature dimensions. Luo et al. [3] used the RGB color components and direction information as block features. Li et al. [4] used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic [5] calculated the 24 Blur-invariant moments as features. Kang and Wei [6] calculated the singular values of a reduced-rank approximation in each block. Bayram et al. [7] used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. [8], [9] used the mean intensities of circles with different radii around the block center to represent the block features. Lin et al. [10] used the gray average results of each block and its sub-blocks as the block features. Ryu et al. [11], [12] used Zernike moments as block features. Bravo-Solorio and Nandi [13] used information entropy as block features.

As an alternative to the block-based methods, keypoint based forgery detection methods were proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In [14]–[16] and [18], the Scale-Invariant Feature Transform (SIFT) [20] was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In [17] and [19], the Speeded Up Robust Features (SURF) [21] were applied to extract features instead of SIFT. However, although these methods can locate the matched keypoints, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate [22].

Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Although these algorithms are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases; 2) the methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Although the existing keypoint-based forgery detection methods can avoid the first two problems, they can reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing keypoint-based forgery methods were very poor.

III. PROPOSED APPROACH

In this paper we propose a very new approach that is combining both the block based and the keypoint based forgery detection approaches (Fig 2). Input image is divided into irregular blocks using adaptive over segmentation. Then feature points were extracted from each image block as a block feature. Then those block features were matched with one another to locate the labeled feature points. To locate the forged region more accurately local color features were extracted and are merged together. **Fig 2: Proposed approach.**


Input Image
Adaptive Over Segmentation
Image Blocks
Block Feature Extraction
Block Features
Adaptive Block Feature Matching
Labeled Feature Points
Forgery Region Extraction
Output: Copy Moved Forged Region

A. ADAPTIVE OVER-SEGMENTATION

Adaptive over segmentation algorithm which is similar to the traditional block based forgery detection methods and can divide the input image into blocks. Of the existing block based forgery detection schemes, the input image was usually divided into overlapping regular blocks with block size being defined and fixed. But in the proposed Adaptive over segmentation method, the input image is divided into non overlapping regions of irregular shape.

Simple Linear Iterative Clustering (SLIC) algorithm is used to segment the input image into meaningful irregular superpixels, as individual blocks. Superpixels are perceptually meaningful atomic regions that can be obtained by over segmentation. Using the SLIC segmentation method, the non overlapping segmentation can decrease the computational expenses compared with the overlapping blocking. Irregular and meaningful region can represent the forgery region more accurately than regular regions.

To obtain initial superpixel value Low Frequency Energy, High Frequency Energy and Percentage of Low Frequency Distribution are calculated. Low Frequency Energy is obtained by calculating the summation of the fourth level of approximation coefficients. High Frequency Energy is obtained by calculating the summation of four levels of detailed coefficients such as horizontal coefficients, vertical coefficients, and diagonal coefficients. If the percentage of Low Frequency Energy is greater than 50% then the input image m*n pixel is multiplied by the scale factor of 0.02. Else if the percentage of Low Frequency Energy is less than or equal to 50% then the input image m*n pixel is multiplied by the scale factor of 0.01. From this Initial size of the superpixel is obtained. Finally SLIC segmentation algorithm together with the calculated initial size S to segment the input image to obtain the image blocks.

- $E_{LF}=\sum|CA_4|$
  Where CA_4 is the 4th level of approximation coefficients.
- $E_{HF} =\sum_i(\sum |CD_i| +\sum |CV_i| +\sum |CH_i|)$

Where i = 1, 2, 3, 4. (Summation of 4 levels of detailed coefficients).

- $P_{LF} = (E_{LF} / (E_{LF} + E_{HF}))*100$
- $S = \sqrt[2]{M*N*0.02}$ if $P_{LF} > 50\%$
- $S = \sqrt[2]{M*N*0.01}$ if $P_{LF} \leq 50\%$

B. BLOCK FEATURE EXTRACTION

Block feature extraction process is employed for the calculation of the similarity between the features extracted from the irregular block regions based on Scale Invariant Feature Transform (SIFT) process. The process identifies the key points from the image blocks. The key points extracted from the irregular blocks were matched based on distance calculated. The derivative of the images is calculated. The calculated values give the changes in the color and the gray scale values of the image which indicates the information in the image.

SIFT is an algorithm to detect and describe local features in images. For any object in an image, interesting points on the object can be extracted to provide a "feature description" of the object. To perform reliable recognition, it is important that the features extracted from the image blocks should be detectable even under changes in the image scale, noise and illumination. Such points usually lie on high-contrast regions of the image, such as object edges.

C. BLOCK FEATURE MATCHING

The block features obtained from the previous step is used to calculate the correlation coefficients of the image blocks. Correlation Coefficients of the image block indicate the number of matched feature points between the corresponding two image blocks. If there were N blocks after adaptive over segmentation (N*(N-1))/2 correlation coefficients can be generated which form the correlation coefficient map. Among the blocks, the two feature points are matched when their Euclidean distance is greater than the predefined feature point matching threshold $TR_{p.}$ TR_p is set to 2 to provide a good trade-off between the matching accuracy and miss probability.

$$d(fa, f_b) \cdot TRp \leq d(f_a, f_i)$$

Where d (fa, f_b) is the Euclidean distance between the feature points f_a and f_b and d(f_a, f_i) is the Euclidean distance between the keypoints f_a and all of the other keypoints in the corresponding block.

$$d(fa, f_b) = \sqrt[2]{(xa-xb)^2 + (ya-yb)^2}$$

$$d(fa, f_i) = \sqrt[2]{(xa-xi)^2 + (ya-yi)^2}$$

Where i = 1, 2, ...n; $i \neq a$, $i \neq b$

Block matching threshold and feature point matching threshold are calculated in order to avoid false matching and improve the accuracy rate in the detection of copy moved forged part.

To calculate the block matching threshold TR_B the first derivative and second derivative of the correlation coefficients as well as the mean value of the first derivative vector are calculated. Minimum correlation coefficient is selected among those whose second derivative is larger than the mean value of the corresponding first derivative vector.

When the correlation coefficient of the block pair is larger than the $TR_{B,}$ the corresponding block pair is determined to be the matched block. The matched feature points in the matched blocks are labeled to indicate the suspected forgery regions. The equation 4.11 indicates that the two feature points were matched when their Euclidean distance is greater than feature point matching threshold in order to avoid false matching among the blocks. With these two block matching threshold and feature point matching threshold most of the false matching can be avoided.

D. FORGERY REGION EXTRACTION

To locate the forgery region more accurately forgery region extraction algorithm is used. Replace the labeled feature points with the small superpixel in order to obtain the suspected regions. To improve the precision and recall results local color feature of the superpixels that are neighbors to the suspected regions are measured. Then merge the neighboring superpixels into the corresponding suspected regions which generate the merged region. Finally, a close morphological operation is applied to the merged region to generate the detected copy-move forgery regions.

For each suspected region $SR_i = \langle LSi, \overline{LSi} \rangle$ the neighboring blocks are defined as $SR_{i\_neighbor} = \langle LSi\_\theta\ , \overline{LSi\_\theta} \rangle$ where θ = {45°, 90°, 135°, 180°, 225°, 270°, 315°, 360°}

$$F_C\_LS = \frac{R(LSi) + G(LSi) + B(LSi)}{3}$$

$$F_C\_\overline{LSi} = \frac{R(\overline{LSi}) + G(\overline{LSi}) + B(\overline{LSi})}{3}$$

$$F_C\_\ LSi\_\theta = \frac{R(LSi\_\theta) + G(LSi\_\theta) + B(LSi\_\theta)}{3}$$

$$F_C\_\overline{LSi\_\theta} = \frac{R(\overline{LSi\_\theta}) + G(\overline{LSi\_\theta}) + B(\overline{LSi\_\theta})}{3}$$

Where R(), G() and B() mean calculating the RGB components of the corresponding block, respectively.

When the local color feature of the neighboring blocks is similar to that of the corresponding suspected regions, which means that the local feature can meet the condition defined as follows,

$|F_C\_LSi - F_C\_\ LSi\_\theta\ | \leq TR_{sim}$

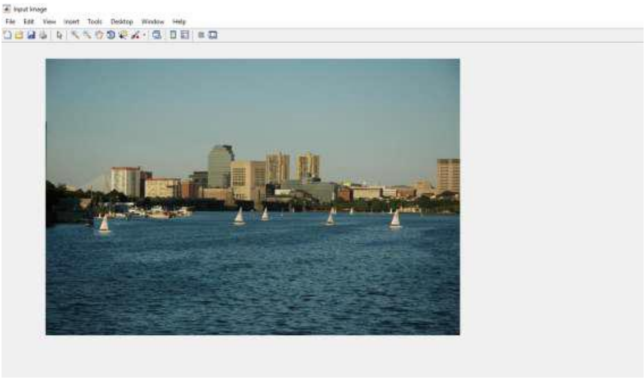
$|\ F_C\_\overline{LSi}\ - F_C\_\overline{LSi\_\theta}\ | \leq TR_{sim}$

The neighboring block will be merged into the corresponding suspected region where F_{C_LSi} and $F_C\_\overline{LSi}$ are the local color features of the corresponding suspected region $SR_i = \langle LSi, \overline{LSi} \rangle$; F_C_LSi and $F_C\_\overline{LSi\_\theta}$ are the local color features of its neighboring blocks $SR_{i\_neighbor}$, $SR_{i\_neighbor} = \langle LSi\_\theta\ , \overline{LSi\_\theta} \rangle$. TR_{sim} is the threshold to measure the similarity between the local color features. Finally, the structural element that is used in the close operation is defined as a circle whose radius is related to the size of the input image. The close operation can fill the gaps in the merged regions and, at the same time, keep the shape of the region unchanged.

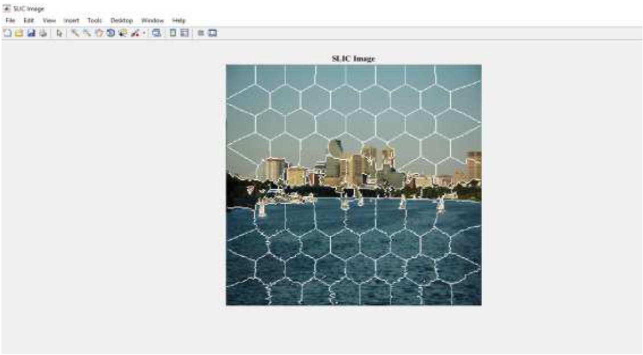
IV. EXPERIMENTAL RESULTS

Figure 4 shows the results for detecting Image Copy-Move Forgery. The original image and the tampered image are shown in figure (a) and (b) respectively. Some part of the original image has been copied to other areas to get the tampered image. Figure (c) is the SLIC segmented tampered image. Figure (d) shows the SIFT Feature extraction for the tampered image. Figure (e) shows the Labeled feature points. Figure (f) shows the detected copy move forged region.

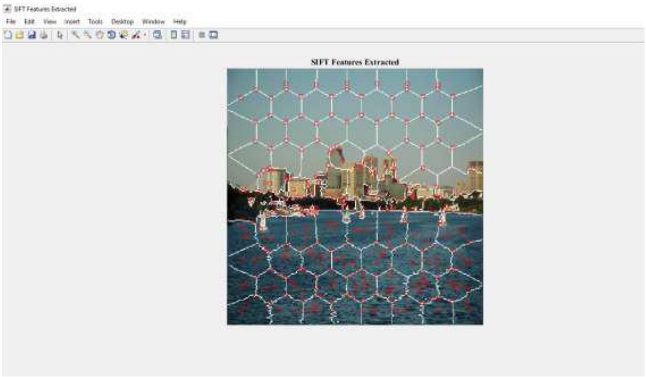
(a)



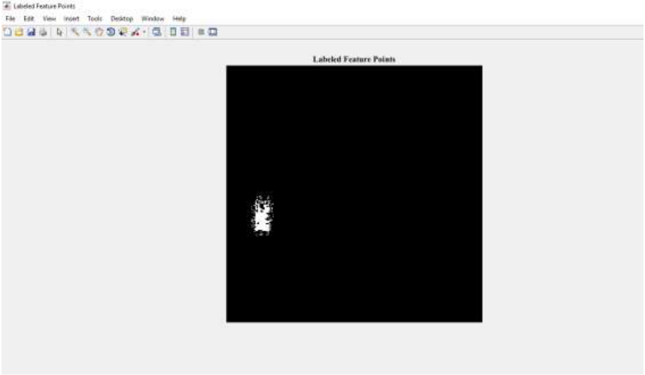
(b)



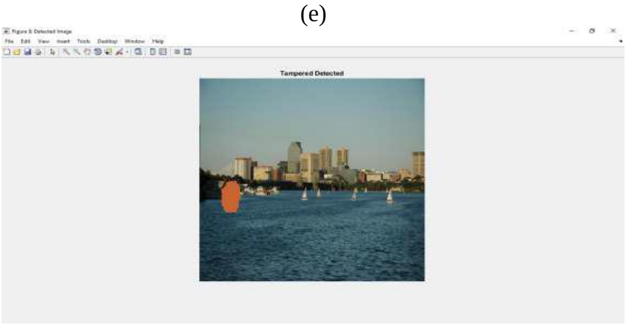
(c)



(d)



(e)



(f)

The table 6.1 depicts that the precision and recall rate of Adaptive Block size is approximately greater than 96 and equal to 100 respectively which is more accurate than the fixed block size, the precision and recall rate is 95.92 and 97.92 respectively.

Table 6.1: Performance Analysis of fixed block size versus adaptive block size.

Method	Precision	Recall
Existing system with fixed block size	95.92	97.92
Proposed system with adaptive block size	96.9	100

V. CONCLUSION

The proposed method is used to find whether the image is Digital forgery images created with copy-move operations are challenging to detect. The Adaptive Over Segmentation algorithm is proposed to segment the input image into non-overlapping and irregular blocks adaptively according to the texture of the input images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labeled feature points are replaced with small superpixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions. The proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms such as scaling, rotation etc than the existing state-of-the-art copy move forgery detection schemes. The performance of the process is calculated with the help of the performance measures like Precision and Recall.

VI. FUTURE WORK

The process can be further improved with the help of the application of different algorithms for the segmentation of the images. The proposed image forgery detection techniques can be applied to other types of forgeries, such as splicing etc. The proposed approach can further applied to other types of media, such as video and audio.

VII. REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy–move forgery in digital images," in *Proc. Digit. Forensic Res. Workshop*, Cleveland, OH, Aug. 2003.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[3] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2006, pp. 746–749.

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2007, pp. 1750–1753.

[5] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic Sci. Int.*, vol. 171,nos. 2–3, pp. 180–189, 2007.

[6] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, Dec. 2008, pp. 926–930.

[7] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy–move forgery," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Apr. 2009, pp. 1053–1056.

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2009, pp. 25–29.

[9] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, "Fast and robust forensics for image region-duplication forgery," *Acta Automat. Sinica*, vol. 35, no. 12, pp. 1488–1495, 2009.

[10] H. J. Lin, C. W. Wang, and Y. T. Kao, "Fast copy–move forgery detection," *WSEAS Trans. Signal Process.*, vol. 5, no. 5, pp. 188–197, 2009.

[11] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding*. Berlin, Germany: Springer-Verlag, 2010, pp. 51–65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments,"*IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1355–1370,Aug. 2013.

[13] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, May 2011, pp. 1880–1883.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of copy–move forgery in digital images using SIFT algorithm," in *Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA)*, Dec. 2008, pp. 272–276.

[15] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[17] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy–move forgery detection based on SURF," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2010, pp. 889–892

[18] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy–move forgery detection based on SURF," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2010, pp. 889–892.

[19] P. Kakar and N. Sudha, "Exposing postprocessed copy–paste forgeries through transform-invariant features," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1018–1028, Jun. 2012.

[20] B. L. Shivakumar and S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," *IJCSI Int. J. Comput. Sci. Issues*, vol. 8, issue 4. no. 1, pp. 199–205, 2011.

[21] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proc. 7th IEEE Int. Conf. Comput. Vis.*, Sep. 1999, pp. 1150–1157.

[22] H. Bay, T. Tuytelaars, and L. Van Gool, "SURF: Speeded up robust features," in *Computer Vision*. Berlin, Germany: Springer-Verlag, 2006, pp. 404–417.

[23] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy–move forgery detection approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[24] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 11, pp. 2274–2282,Nov. 2012.