Research Article

Region Duplication Forgery Detection Technique Based on SURF and HAC

Parul Mishra,¹ Nishchol Mishra,¹ Sanjeev Sharma,¹ and Ravindra Patel²

¹ School of Information Technology, RGPV, Bhopal, Madhya Pradesh 462036, India

² University Institute of Technology, RGPV, Bhopal, Madhya Pradesh 462036, India

Correspondence should be addressed to Parul Mishra; parul123_mishra@yahoo.com

Received 16 August 2013; Accepted 17 September 2013

Academic Editors: H. Cheng, H.-E. Tseng, and Y. Zhang

Copyright © 2013 Parul Mishra et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Region duplication forgery detection is a special type of forgery detection approach and widely used research topic under digital image forensics. In copy move forgery, a specific area is copied and then pasted into any other region of the image. Due to the availability of sophisticated image processing tools, it becomes very hard to detect forgery with naked eyes. From the forged region of an image no visual clues are often detected. For making the tampering more robust, various transformations like scaling, rotation, illumination changes, JPEG compression, noise addition, gamma correction, and blurring are applied. So there is a need for a method which performs efficiently in the presence of all such attacks. This paper presents a detection method based on speeded up robust features (SURF) and hierarchical agglomerative clustering (HAC). SURF detects the keypoints and their corresponding features. From these sets of keypoints, grouping is performed on the matched keypoints by HAC that shows copied and pasted regions.

1. Introduction

Today, the use of digital images is increasing rapidly in almost every area of human life like in education, software companies, television, businesses, journalism, medical imaging, and social media. It is easy to learn and understand anything visually rather than only reading or listening. Another aspect is that generally visual information is believed to be true. But as the technology advances and lots of sophisticated image processing tools are available, it becomes very easy to edit visual information. Some of the tools are *Adobe Photoshop*, *GIMP*, *Macromedia Freehand*, and *Corel Paint Shop* [1, 2]. A big question arises, how to distinguish the photographic images from the photorealistic ones [3].

Digital image forensic is a branch that deals with crimes, where images are used as a prime evidence in the court of law. Forensic sciences have methods to identify the source device, for example, camera, scanner, and so forth, with their particular model. If any tampering is done on the image then it can also be detected. Tampering an image means either adding or removing some information from an image, so that the original meaning will be changed [4].

If the alteration is intentional and related with some kind of benefits, it can be termed as a digital image forgery. Forgery detection methods are mainly divided into two different categories: *active* and *passive*. In active method, some information for example digital watermark or digital signature is preembedded into the image. This procedure is performed for the sake of providing authenticity to an image. But the images distributed on the web do not contain always preembedding information. To overcome the drawback of active methods, passive methods have been developed [5]. The tampering again is of two types either it is performed on the same image or on multiple images. If some area is copied and pasted into another area of the same image, it is known as *copy move forgery* or *region duplication forgery*. When two or more images are involved and their combination produces a fake image then it is called *splicing* or *photomontage* [6]. Farid gives lots of examples of real incidents with image forgery [7]. On July 2008, a forged image of four Iranian missiles was posted on the web and published in newspapers [8]. Egypt's newspaper *Al-Ahram* on Sept. 2010 published a forged image. In this image president Mubarak was leading the group instead of Barak

FIGURE 1: Classification of copy move forgery detection techniques.

Obama at the White House, during Middle East peace talks [9].

The rest of the paper is organized as follows: Section 2 presents the related work; Section 3 describes the proposed method for duplicate detection. The results of forgery detection by experimental evaluation are presented in Section 4, and Section 5 describes the conclusion of the paper.

2. Related Work

In region duplication detection, the forged region can be identified by applying proper detection techniques. These techniques are classified into block based and keypoint based methods [10]. The classification of duplication detection methods is illustrated in Figure 1.

2.1. Block Based Methods. In this approach, an image is divided into different overlapping blocks of fixed size; it is assumed that the block size is smaller than the duplicated region. After dividing the image into different block sizes, features are extracted from it by applying different methods. These features are then matched with other features of each block. A match indicates the probability of forgery. Fridrich et al. [11] discuss the exhaustive search and autocorrelation of forgery detection. Furthermore, they applied discrete cosine transform (DCT) on each separate block. DCT is applied from the upper left corner to the bottom right corner. For reducing the computation, features are extracted from the low frequency component. In this method, feature dimension size is 64.

Popescu and Farid [12] presented a method based on principal component analysis (PCA) that reduces the dimensional size to 32. Extracted features are lexicographically sorted; therefore, matched features come closer to each other. This method is robust towards compression and additive noise. Bayram et al. [13] proposed Fourier Mellin transforms (FMT) for copy move forgery detection. Features extracted

are of length 45, and they are rotation invariant only to some degree. Bloom filter was used here instead of lexicographical sorting, which reduces the detection time.

Moment invariant features are insensitive towards all transformation; hence, it can be used to detect the region duplication. Blur moment invariant detects the forgery in the presence of blur degradation, and its performance remains unaffected by additive zero mean noise. Each separate block is represented by a feature vector whose dimension length is 24 in case of gray level. The KD tree method is applied here for nearest neighbour searching, and then similar blocks denote the duplicated regions [14]. Ryu et al. [15] proposed a method which utilizes rotation invariant Zernike moment. It also gives significant performance in case of JPEG compression, blurring, and noise contamination. In [16], the authors applied Gaussian pyramid on image to decompose it into different scales. After that each scale space is divided into separate circular blocks. From each circular block features are extracted by Hu moment of length 4. Features are then sorted, and matching is performed on it. The performance of this method is not changed in the presence of a rotational transformation.

Li et al. [17] applied discrete wavelet transform (DWT) and singular value decomposition (SVD) to the image. Firstly, DWT is applied to each block that reduces the size of the block. Then, SVD is applied on low frequency components, which reduce the feature dimensional size to 4. After that features are lexicographically sorted and matched. In [18], the image is divided into overlapping patches. Features are extracted from each patch by applying PCT. PCT utilizes the orthogonal properties so that features of PCT are more compact. It is a rotational invariant method and also performs better in the presence of noise.

Bravo-Solorio and Nandi [19] mapped all the pixels of overlapping blocks into log polar coordinates. Then, angle orientation creates a 1D descriptor, by doing this synchronization problem can be removed. Feature vectors are calculated from particular blocks depending on the colour and luminance factor. This method is robust towards reflection, rotation, and scale changes.

2.2. Keypoints Based Methods. In this approach, various keypoints are selected from an image. Feature descriptors are calculated from each of these keypoints. For detecting the duplication, forgery matching is performed on keypoint feature descriptors. Lowe [20] invented SIFT, which detects keypoints and features from an image. SIFT application exists in various fields. It performs better in comparison to previous descriptors [21].

In [22], SIFT is applied into the region duplication detection method. In [23], the authors suggested that the keypoint matching method suffers from some problems. For removing these problems, SIFT cluster matching is proposed, where objects are matched rather than the point. Points are grouped here using agglomerative hierarchical clustering.

Pan and Lyu [24] also applied SIFT in their work. For avoiding search from close adjacency, search is applied far from 11×11 pixel window whose center is at the keypoint.

They also applied Random Sample Consensus (RANSAC) for affine transformation detection.

Amerini et al. [25] detect the duplication forgery and also estimate the transformation by RANSAC. They developed g2NN nearest neighbour searching for multiple copy paste detection. Their method is robust to all transformation attacks. Their procedure also works effectively for splicing attack detection. The similar work is done in [26] where the authors used MPEG7 image signature tools for extracting the features. Least Median of Squares (LMedS) algorithm is used instead of RANSAC for estimating the geometrical transformations. Recently Amerini et al. [27] proposed J linkage for effective clustering. In [28], the authors applied resampling traces with SIFT to distinguish the original region from the pasted region in a tamper image. SIFT ring descriptors are applied to an image for detecting the tampering. The size of feature dimension is reduced to 24 from 128 that increases the speed. These feature descriptors are rotationally invariant [29]. SURF is another keypoint based method, which detects 64 feature descriptors. Obtained keypoints are divided into two subsets. Matching procedure is applied and repeated until one keypoint remains in a set [30]. In [31], SURF with KD tree method are used for the detection of a particular forged region. In this proposed work, HAC method is applied with SURF for a more accurate result in terms of all attacks.

3. Proposed Method

This proposed method is based on a SURF algorithm for the detection of keypoints and for extracting their corresponding feature descriptors. Matching is performed in between selected keypoints by applying best bin first search procedure.

For detecting the duplicated regions, HAC technique is applied. The whole procedure of proposed work is depicted in Figure 2, and the related algorithm for detection method is described in Section 3.1. An input image is inserted to the detection system, and the output is imaged with duplicated regions, if it is forged. The first block of the detection framework is keypoint detection and feature extraction that will be explained in Section 3.2. After that matching is performed among selected keypoints, the procedure for keypoint matching will be described in Section 3.3. At last clustering algorithm is applied on the matched keypoints, which will be explained in Section 3.4.

3.1. Region Duplication Detection Algorithm. If the image suffers from duplication forgery, then it contains at least two same regions, one is copied and the other is pasted region. The overall technique for detecting the duplicated region is as follows.

Input: image.

Output: detected duplicate regions with image.

- (1) If RGB image, then converted into gray scale.
- (2) Applying SURF method.

- (a) Keypoints are detected from an image $(1, 2, 3, \dots, M)$.

- (b) From the above detected keypoints, features are extracted $(N_1, N_2, N_3, \dots, N_M)$.
- (c) This matrix is stored in a variable $D = M \times N$.

- (3) For each $i = 1$ to M ,
for $j = 1$ to M .

- (a) If $i \neq j$, then go to step (b); else: return.
- (b) Dot products are calculated between each feature descriptor.

End of For j .

- (c) Inverse cosine angle of dot products will be computed.
- (d) Sorting is applied on the result, and values are stored

[Value, index] = sort ($\cos^{-1}(\text{dot prods})$).

- (e) If (Value(1)/Value(2)) < 0.6, then match exists, and index will be stored.

Else: index = 0.

End of For i .

- (4) For each keypoint

- (a) If match exists, then go to step (b);

else: return.

- (b) If the matched points are far from 10×10 square region, then go to step (c);

else: return.

- (c) Store the coordinates of matched points in m by n data matrix X and set: flag = 1.

End of For.

- (5) If flag > 0, then

- (a) euclidean distance computed between each pair of objects of X ;

$$\text{Dist } (A, B) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}; \quad (1)$$

where, $A = (x_1, y_1)$, $B = (x_2, y_2)$

- (b) linkage function is applied for linking the objects into hierarchal tree;
- (c) the smallest height is taken for cutting the hierarchal tree into clusters;
- (d) a line is drawn between the matched objects from different clusters;
- (e) objects of different clusters are shown from the different colours.

FIGURE 2: Flow chart of proposed work.

FIGURE 3: Integral image calculation by rectangular region.

3.2. Keypoint Detection and Feature Extraction. Bay et al. [32] proposed SURF method whose computation is faster than SIFT. How keypoints are detected and feature descriptor is generated from SURF are discussed below.

3.2.1. Integral Image. Integral image increases the computation speed as well as the performance, its value is calculated from an upright rectangular area.

In Figure 3, the sum of all pixel intensities is calculated by the formula, which is written in the rectangular area whose

vertices are A, B, C , and D . Suppose that an input image I and a point $(x; y)$ are given. The integral image I_{Σ} is calculated by the sum of the values between the point and the origin. The following formula is used to calculate the integral image:

$$I_{\Sigma}(x, y) = \sum_{i=0}^{x-1} \sum_{j=0}^{y-1} I(x, y). \quad (2)$$

3.2.2. Keypoint Detection. This step requires scale space generation for the extraction of keypoints. In SURF, Laplacian of Gaussian is approximated with a box filter. Convolution is applied to an image with varying size box filter for creating the scale space. After constructing the scale space, determinant of the Hessian matrix is calculated for detecting the extremum point. If determinant of the Hessian matrix is positive, that means both the Eigen values are of the same sign either both are negative or both are positive. In case of the positive response, points will be taken as extrema; otherwise, it will be discarded.

Hessian matrix is represented by

$$H(x, y) = \begin{bmatrix} L_{xx}(x, y) & L_{xy}(x, y) \\ L_{xy}(x, y) & L_{yy}(x, y) \end{bmatrix}, \quad (3)$$

where $L_{xx}(x, \sigma)$ is the convolution of the Gaussian second order derivative with the image I in point x , and similarly $L_{xy}(x, \sigma)$ and $L_{yy}(x, \sigma)$. These derivatives are called Laplacian of Gaussian. The approximate determinant of the Hessian matrix is calculated by

$$\det(H_{\text{approx}}) = D_{xx}D_{yy} - (0.9D_{xy})^2. \quad (4)$$

3.2.3. Orientation Assignment. At first, a circular area is constructed around the keypoints. Then, Haar wavelets are used for the orientation assignment. It also increases the robustness and decreases the computational cost. Haar wavelets are filters that detect the gradients in x and y directions. In order to make rotation invariant, a reproducible orientation for the interest point is identified. A circle segment of 60° is rotated around the interest point. The maximum value is chosen as a dominant orientation for that particular point.

3.2.4. Feature Descriptor Generation. For generating the descriptors, first construct a square region around an interest point, where interest point is taken as the center point. This square area is again divided into 4×4 smaller subareas. For each of these cells, Haar wavelet responses are calculated. Here, d_x termed as horizontal response and d_y as vertical response. For each of these subregions, 4 responses are collected as

$$v_{\text{subregion}} = [\sum dx, \sum dy, \sum |dx|, \sum |dy|]. \quad (5)$$

So each subregion contributes 4 values. Therefore, the descriptor is calculated as $4 \times 4 \times 4 = 64$.

3.3. Keypoint Matching. A set of keypoints and their corresponding feature descriptors are obtained from SURF. The comparison is performed between each keypoint with the remaining other keypoints feature descriptor. As matching these keypoints with their high dimensional feature vector 64 takes time, therefore best bin first (BBF) method is chosen for selecting two nearest neighbours [33]. Dot products are calculated between each keypoint feature descriptor with the others. After that sort the inverse cosine angles of dot products. Store their values as well as their corresponding index number. The ratio between two nearest neighbours value is compared to a predefined threshold. In this work, the threshold is set to 0.6, because above this value the probability of false matches arises. If the ratio is less than the given threshold, they satisfy the similarity criterion and match exists. In case of matching, their relative index number will be stored. This procedure continues for all keypoints.

3.4. Keypoint Clustering. HAC is also known as hierarchy of clusters, in which each keypoint behaves as a single cluster at the starting stage. Euclidean distance between each keypoint with the remaining other keypoints will be calculated. Merging is performed if two clusters are dissimilar to each other. This step is repeated until there is one cluster left or dissimilarity criterion unsatisfied [34]. Single, average,

and ward methods are types of linkage used for merging and creating a hierarchal tree.

Single Linkage. It uses the smallest distance between objects in two clusters,

$$d(A, B) = \min(\text{dist}(x_{A_i}, x_{B_j})). \quad (6)$$

Average Linkage. It uses the average distance between all pairs of objects in the two clusters,

$$d(A, B) = \frac{1}{n_A n_B} \sum_{i=1}^{n_A} \sum_{j=1}^{n_B} \text{dist}(x_{A_i}, x_{B_j}). \quad (7)$$

Ward Linkage. It is based on the increment or decrement in the value of error sum of squares (ESS). In other words, distance between the clusters is the difference between the ESS for unified cluster and ESS of the individual clusters,

$$d(A, B) = \text{ESS}(AB) - [\text{ESS}(A) + \text{ESS}(B)], \quad (8)$$

where

$$\text{ESS}(A) = \sum_{i=1}^{n_A} |x_{A_i} - \bar{x}_A|^2. \quad (9)$$

Here, AB indicates the combined cluster, n_A indicates number of objects in cluster A , n_B indicates number of objects in cluster B , x_{A_i} indicates i th object in the cluster A , and $\bar{x}_A$ indicates centroids of cluster whose value is calculated by

$$\bar{x}_A = \frac{1}{n_A} \sum_{i=1}^{n_A} x_{A_i}. \quad (10)$$

4. Experimental Results

In this section, experiment of duplication detection is performed on the MICC-F220 dataset [35]. This dataset contains 220 images, from them 110 are real and 110 are fake. 10 different combinations of scaling and rotation attacks are already applied to each forged image of the dataset [25]. Images shown in Figure 4 represent the detection results in the presence of various scaling and rotation attacks.

For checking the robustness of this method we applied different attacks on images. Figure 5 depicts the detection result in the presence of compression, for JPEG quality factor 20, 40, 60, and 80, respectively. Figure 6 denotes the detection results in addition of white Gaussian noise whose SNR values are 20, 30, 40, and 50, respectively. In Figure 7, detection results are shown in the presence of Gaussian blurring. The value of the window size is 5×5 , 7×7 , and the value of σ is taken as 0.5, 1. Figure 8 represents the detection results in the presence of Gamma correction values 1.2, 1.4, 1.6, and 1.8. In all these images, copied and pasted regions are represented separately by clusters. A line drawn between two key points indicates that this point matches with each other.

FIGURE 4: Copy paste detection results in the presence of 10 different rotation and scaling attacks applied on the image.

FIGURE 5: Copy paste detection results for compression: (a) JPEG image quality factor 20, (b) JPEG image quality factor 40, (c) JPEG image quality factor 60, and (d) JPEG image quality factor 80.

FIGURE 6: Copy paste detection results for noise addition: (a) SNR value 20, (b) SNR value 30, (c) SNR value 40, and (d) SNR value 50.

FIGURE 7: Copy paste detection results for blurring: (a) window size 5×5 , $\sigma = 0.5$, (b) window size 5×5 , $\sigma = 1$, (c) window size 7×7 , $\sigma = 0.5$, and (d) window size 7×7 , $\sigma = 1$.

FIGURE 8: Copy paste detection results for: (a) gamma value = 1.2, (b) gamma value = 1.4, (c) gamma value = 1.6, and (d) gamma value = 1.8.

TABLE 1: TPR, FPR values (%) and processing time (average per image) for each method.

Methods	FPR%	TPR%	Time (s)
Fridrich et al. [11]	84	89	294.69
Popescu and Farid [12]	86	87	70.97
Amerini et al. [25]	8	100	4.94
SURF and HAC	3.64	73.64	2.85

The performance of detection method is measured in terms of true positive rate (TPR), false positive rate (FPR), and time complexity where

$$TPR = \frac{\text{images detected as forged being forged}}{\text{total number of forged images}}, \quad (11)$$

$$FPR = \frac{\text{images detected as forged being original}}{\text{total number of original images}}. \quad (12)$$

TPR is the percentage of forged images, which are correctly identified. FPR is the percentage of the original image which is wrongly identified as a tampered.

The values of FPR, TPR, and time (in seconds) for SURF and HAC methods will be computed. Then, a comparison is performed with other methods. The starting three rows shown in Table 1 are taken from [25] as a benchmark and the fourth row represents the value obtained from SURF and HAC based methods. Figure 9 represents the result in graphical form. The graph indicates that this method reduces the FPR rate as well as the time complexity. FPR value is approximately 4, which is lower than DCT [11] and PCA [12] methods. Also, the time required to detect the forgery is very low compared to [11] and [12]. TPR value is low which shows one drawback of this method.

5. Conclusion and Future Work

In this paper, a method was presented for detecting the duplicate region based on SURF and HAC. The integral image used in SURF reduces the time complexity. SURF has less feature descriptor dimensional size. So that matching applied on SURF descriptor is faster and increases the computation speed as well. The Haar wavelets are used for feature descriptors computation from each keypoint, so descriptors are robust to illumination changes. The experimental results

FIGURE 9: Performance of the methods represented in graph.

show that SURF feature descriptors are invariant towards different combination of scaling and rotation. In the presence of JPEG compression, Gaussian noise addition and gamma correction attack; this method gives good result. HAC is used here for creating the regions from matched keypoints. HAC is easy to implement and create regions in less time, but satisfactory result is not obtained in terms of the true positive rate. So in the future we would like to replace clustering with suitable image segmentation technique, also we want to utilize this method for multiple duplication detection in a single image.

Conflict of Interests

The authors declares that there is no conflict of interests regarding the publication of this paper.

References

- [1] S. Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in *Proceedings of the IEEE Western New York Image Processing Workshop*, pp. 538–542, September 2008.
- [2] W. Luo, Z. Qu, F. Pan, and J. Huang, "A survey of passive technology for digital image forensics," *Frontiers of Computer Science in China*, vol. 1, no. 2, pp. 166–179, 2007.

- [3] S. Lyu and H. Farid, "How realistic is photorealistic?" *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 845–850, 2005.
- [4] J. A. Redi, W. Taktak, and J. Dugelay, "Digital image forensics: a booklet for beginners," *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 133–162, 2011.
- [5] H. Farid, "Image forgery detection," *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16–25, 2009.
- [6] M. Sridevi, C. Mala, and S. Sanyam, "Comparative study of image forgery and copy-move techniques," in *Advances in Computer Science, Engineering & Applications*, pp. 715–723, Springer, Berlin, Germany, 2012.
- [7] H. Farid, "Seeing is not believing," *IEEE Spectrum*, vol. 46, no. 8, pp. 44–51, 2009.
- [8] M. Nizza and P. J. Lyons, *In an Iranian Image, A Missile Too Many. The Lede*, News Blog, The New York Times, New York, NY, USA, 2008.
- [9] S. D. Mahalakshmi, K. Vijayalakshmi, and S. Priyadharsini, "Digital image forgery detection and estimation by exploring basic image manipulations," *Digital Investigation*, vol. 8, no. 3, pp. 215–225, 2012.
- [10] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012.
- [11] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, Cleveland, Ohio, USA, August 2003.
- [12] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, 2004.
- [13] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 1053–1056, IEEE, April 2009.
- [14] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," *Forensic Science International*, vol. 171, no. 2, pp. 180–189, 2007.
- [15] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding*, pp. 51–65, Springer, Berlin, Germany, 2010.
- [16] G. Liu, J. Wang, S. Lian, and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Journal of Network and Computer Applications*, vol. 34, no. 5, pp. 1557–1565, 2011.
- [17] 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 *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07)*, pp. 1750–1753, IEEE, July 2007.
- [18] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," *Forensic Science International*, vol. 224, pp. 159–367, 2012.
- [19] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics," *Signal Processing*, vol. 91, no. 8, pp. 1759–1770, 2011.
- [20] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.
- [21] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 10, pp. 1615–1630, 2005.
- [22] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using sift algorithm," in *Proceedings of the Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA '08)*, vol. 2, pp. 272–276, IEEE, December 2008.
- [23] E. Ardizzone, A. Bruno, and G. Mazzola, "Detecting multiple copies in tampered images," in *Proceedings of the 17th IEEE International Conference on Image Processing (ICIP '10)*, pp. 2117–2120, IEEE, September 2010.
- [24] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 857–867, 2010.
- [25] 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 Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.
- [26] P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform-invariant features," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 1018–1028, 2012.
- [27] I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, L. del Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-linkage," *Signal Processing*, vol. 28, no. 6, pp. 659–669, 2013.
- [28] D. Vázquez-Padín and F. Pérez-González, "Exposing original and duplicated regions using SIFT features and resampling traces," in *Digital Forensics and Watermarking*, pp. 306–320, Springer, Berlin, Germany, 2012.
- [29] L. N. Zhou, Y. B. Guo, and X. G. You, "Blind copy-paste detection using improved SIFT ring descriptor," in *Digital Forensics and Watermarking*, pp. 257–267, Springer, Berlin, Germany, 2012.
- [30] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *Proceedings of the 2nd International Conference on Multimedia Information Networking and Security (MINES '10)*, pp. 889–892, IEEE, November 2010.
- [31] B. L. Shivakumar and S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," *International Journal of Computer Science Issues*, vol. 8, no. 4, p. 199, 2011.
- [32] H. Bay, T. Tuytelaars, and L. van Gool, "Surf: speeded up robust features," in *Computer Vision-ECCV, 2006*, pp. 404–417, Springer, Berlin, Germany, 2006.
- [33] J. S. Beis and D. G. Lowe, "Shape indexing using approximate nearest-neighbour search in high-dimensional spaces," in *Proceedings of the 1997 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1000–1006, June 1997.
- [34] T. Hastie, R. Tibshirani, and J. J. H. Friedman, *The Elements of Statistical Learning. Volume 1*, Springer, New York, NY, USA, 2001.
- [35] <http://www.micc.unifi.it/ballan/research/image-forensics/>.