Journal of Computer and Communications, 2019, 7, 1-18
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Copy-Move Forgeries Detection and Localization Using Two Levels of Keypoints Extraction

Soad Samir*, Eid Emary, Khaled Elsayed, Hoda Onsi

Faculty of Computers and Information, Cairo University, Giza, Egypt
Email: *soad.samir@hotmail.com, eid.emary@aou.edu.eg, k.mostafa@fci-cu.edu.eg, h.onsi@fci-cu.edu.eg

How to cite this paper: Samir, S., Emary, E., Elsayed, K. and Onsi, H. (2019) Copy-Move Forgeries Detection and Localization Using Two Levels of Keypoints Extraction. *Journal of Computer and Communications*, **7**, 1-18.
https://doi.org/10.4236/jcc.2019.79001

Received: August 8, 2019
Accepted: September 1, 2019
Published: September 4, 2019

Abstract

Copy-move offense is considerably used to conceal or hide several data in the digital image for specific aim, and onto this offense some portion of the genuine image is reduplicated and pasted in the same image. Therefore, Copy-Move forgery is a very significant problem and active research area to check the confirmation of the image. In this paper, a system for Copy Move Forgery detection is proposed. The proposed system is composed of two stages: one is called the detection stages and the second is called the refine detection stage. The detection stage is executed using Speeded-Up Robust Feature (SURF) and Binary Robust Invariant Scalable Keypoints (BRISK) for feature detection and in the refine detection stage, image registration using non-linear transformation is used to enhance detection efficiency. Initially, the genuine image is picked, and then both SURF and BRISK feature extractions are used in parallel to detect the interest keypoints. This gives an appropriate number of interest points and gives the assurance for finding the majority of the manipulated regions. RANSAC is employed to find the superior group of matches to differentiate the manipulated parts. Then, non-linear transformation between the best-matched sets from both extraction features is used as an optimization to get the best-matched set and detect the copied regions. A number of numerical experiments performed using many benchmark datasets such as, the CASIA v2.0, MICC-220, MICC-F600 and MICC-F2000 datasets. With the proposed algorithm, an overall average detection accuracy of 95.33% is obtained for evaluation carried out with the aforementioned databases. Forgery detection achieved True Positive Rate of 97.4% for tampered images with object translation, different degree of rotation and enlargement. Thus, results from different datasets have been set, proving that the proposed algorithm can individuate the altered areas, with high reliability and dealing with multiple cloning.

Keywords

Copy Move Forgery Detection, Keypoint Based Methods, SURF, BRISK, Bi-Cubic Interpolation

1. Introduction

Recently, due to the augmentation in the image processing software applications like Photoshop, GIMP [1] (GNU Image Manipulation Program), NIK collection [2] (offered by Google) and many others software and the simplicity of using these applications, the probability of maleficent modification on the images has also enlarged. The aim of the digital images editing can be to secrete or conceal some data from the genuine image, to raise the image quality, and to pick the more data from two or more images into one image. Three forgeries classes can be recognized on the base of the technique took on to do the forgery [3]. Digital images can be processed in a neatness way, which makes forgery cannot be recognized by human eyes. As a result, the security interest of the digital images information has become apparent a long time ago and many several techniques have been improved to check the authentication of the digital image [4]. Digital image forgeries can be grouped into three major categories and described below:

1) Copy-Move Forgery: a method where a certain part of the genuine image is copied and pasted into the target place in the same image [5].

2) Image Splicing: a method which utilizes cut and paste techniques from different images to create a new fake image [5].

3) Image Retouching: a method that is the least dangerous techniques as compared to the other forgery techniques. Some enhancement of some features of the genuine image is done, and the content of the image stays almost the same [6].

In a copy-move forgery (CMF), one region is simply copied and pasted over the other regions in the same image for manipulating the image. This copy-move is considered as one of the highly popular techniques, in which an area is copied one or more times to give diverse information about the same image, which can be treated as a problem of information fidelity. **Figure 1** shows an example of how to apply CMF in digital images [7]. For the examples presented in the first column, the plant is multiplied to generate contents that do not exist in the genuine image. In the second instance, an area is regenerated to secrete undesirable object (large size stone) in the genuine image. The tampered areas shown in **Figure 1** are well intermingled at the required positions, and get extremely hard to distinguish through the one eye.

Keypoint-based technique is broadly used to find CMF, that is because their robust execution against various counter-forensic post-processing; therefore, many counter-forensics algorithms are presented for keypoint-based. Although keypoint-based is research of interests in digital forensics and is broadly used to

Figure 1. Image forgery examples [8].

find CMF, it may create false detection results when the cloned regions of test image are too small or too smooth, because it is difficult to detect keypoints from such regions with the keypoint-based technology. This issue seriously limits the applications of keypoint-based technology and leads to the lack of authority for detection results because it is difficult to make sure that the test image is not the CMF one, when none of cloned region is pointed out by keypoint-based technology. There are already several feature detection algorithms that have been recommended but the SIFT (Scale Invariant Feature Transform), SURF, BRIEF (Binary Robust Independent Elementary Features), and BRISK are the most auspicious since they perform better and are already used by many researchers and applied in many applications.

The core problem is that the keypoints in small or smooth cloned regions are insufficient or even none. The technique used in [9] can dramatically increase the number of keypoints detected in the entire image by adapting the detection variables of keypoint-based technique. Overall; keypoint-matching consumes a lot of time and memory.

To solve these issues, a novel CMF detection algorithm based on two levels of keypoint extraction and image registration is proposed in this paper. The proposed solution performs CMF detection with two stages. The aim of the first stage is to detach the smooth, and the rough regions of study image. In this stage, SURF and BRISK based schemes are applied to detect the interesting keypoints features from the study image and finding the best match sets from the image. Then in the second stage, the image registration using non-linear transformation is applied to detect the correct best matched pairs and correctly locates the

forged areas. We then compare the performance of the proposed scheme with another similar work using the same keypoints extractions features (BRISK and SURF). Experimental results show that the accuracy of our proposed algorithm is 3% more accurate than similar work presented. Its score is also outperformed the similar work by 2.5%. The results also show that the proposed algorithm doesn't degrade the quality of the detected region and has a low false detection rate comparing to the similar work.

The rest of the paper is organized as follows. In Section 2, we discuss the related work which has been proposed yet with their merits and demerits. In Section 3, the proposed technique is discussed in details. Then we present the detailed experimentation results in Section 4. In Section 5, we draw the conclusion of the paper and future work.

2. Related Work

The key-point based techniques use two step procedures of detecting and describing the interest keypoints. In the first step, localization is carried out and the interest keypoints are described in the second step. Robust descriptors must be invariant to affine transformations. Keypoints based method's execution is comparatively higher than the block based and brute force methods in terms of computational efficiency, complexity, and robustness against various transformations like scaling, rotation, cropping, illuminations, trimming, variations etc.

There are many keypoints based techniques have been proposed to detect the CMF in the tampered image. Some of them are listed below to summarize literature about the keypoints extraction and detection in CMF forged images.

The SURF algorithm had been proposed and deployed by Bay *et al*. [10] in 2006 to enhance the efficiency of SIFT. SURF is fast and robust feature detector. SURF speed is increased due to the integral image. SURF is invariant to scaling and rotation transformations. SURF detector algorithm is not proper for discovering the regions' repetition in case of extremely compressed JPEG images and smooth copied regions. It is proper for non-flat regions. SURF algorithm is one of the major commonly used feature extraction algorithms because it can provide stable visual points called interest points, which are scale invariant and robust under a broad area of view and illustration changes. SURF provides comparable keypoints performance extraction and increased operating speed. Thus; SURF has been pulling a lot of concern in these days. They explained that SURF can minimize the false match specifically for the highly resolution images, whilst robust to specific transformation and post processing processes. However; SURF cannot detect a tiny copied area in the image. It was later shown that the SURF-based technique reduced the accuracy although it improves the processing time in copy-move detection.

Stefan Leutenegger *et al*. [11] proposed a novel high-quality and fast keypoint detection called "BRISK" algorithm. The algorithm is rotation invariant and scale invariant to a high level. It accomplishes high performance, and minimizes computational cost.

Sunil Kumar [12] proposed a technique to detect forgery in images where SURF features are used for keypoints detection and BRISK is used for keypoints description. The proposed technique is invariant to rotation, translation, scaling and geometrical transformations. The matching step is carried out using KNN search hamming distance. The keypoints are detected by SURF, and then extract BRISK features at these keypoints. The KNN search is used for the similarity matching of the BRISK binary features. The nearest neighbor is found using the hamming distance. ***The disadvantages of this method*** are:

1) *It cannot work perfectly at the smooth forged regions, so it cannot detect these regions correctly.*

2) *This method also gives an over-detection rate which gives a high false detection rate.*

Joseph A. Ojeniyi [13] proposed a technique to detect copy move by hybridizing block-based DCT technique and, a keypoint-based SURF technique. In this technique, DCT is applied to the forged image with the main objective of enhancing the detection rate accuracy of the forged image, and then SURF is applied to the generating image with the core objective of detecting forged regions that have been tampered in the image. Efficiency of the hybridized technique had been shown that its detection rate and accuracy is far higher than the previously available methods. The goal of hybridizing both techniques is to be able to compensate the lapses found in each of the techniques. The hybridize technique has a better accuracy rate and it is robust to most of the attacks and preprocessing techniques that are associated with CMF.

Neema Antony *et al.* [14] proposed a method to detect copy move by adaptive over segmentation. The method splits the input forged image into non-overlapping and infrequent blocks adaptively. Using SIFT, the feature key-points are extracted from each blocks. After that, the feature keypoints are matched with one another using brute force matching method. The leading advantage of this method is that it merges block-based and keypoint based methods. So; it enhances the performance of the copy-move image forgery detection and overcomes the limitations of existing block based methods. Experimental result shows that proposed method was effectively detected the copy-move forgery with minimum false match.

Pooja Devi *et al.* [15] proposed a technique to detect picture replica circulate forgery that is depended on SIFT feature. Clustering algorithm is used for clustering of key points in images. This method is a robust method in detecting the copymove forgery quickly and withstands certain transformations.

3. The Proposed Technique

In this section, the CMFD (Copy Move Forgery Detection) has been matured. An efficient keypoint based CMFD technique is proposed. The proposed technique is executed by two stages of detection:

1) The first stage is called the detection stage.

2) The second stage is called refine detection stage.

In the detection stage, the detection is done by the parallelism of two commonly used CMFD, which are BRISK and SURF techniques. The goal of the parallelism of both techniques is to enhance the detection accuracy of CMF from the issues of scaling, rotation, smoothed flat regions for both better detection performance.

In the refine detection stage, we used image registration using bi-cubic interpolation between the results from SURF and BRISK that is done in the detection stage with a view to make hybridization between SURF and BRISK to enhance the detection results and its efficiency.

The results obtained from the proposed technique is been compared with other related work results obtained. We first present the detailed description of the keypoints extraction techniques exploited in this paper, followed by the algorithm framework of the proposed technique for image copy move forgery detection. The flow chart of the whole technique is presented in Figure 2.

3.1. The Detection Stage

In the Detection Stage, we are using SURF keypoints detection in parallel with BRISK keypoint detection. Both algorithms are supported by RANSAC as an outliers' removal to minimize the false detection of forgeries. In the next subsections we will discuss how to use SURF and BRISK as a keypoints feature extractors of forgery detection algorithm.

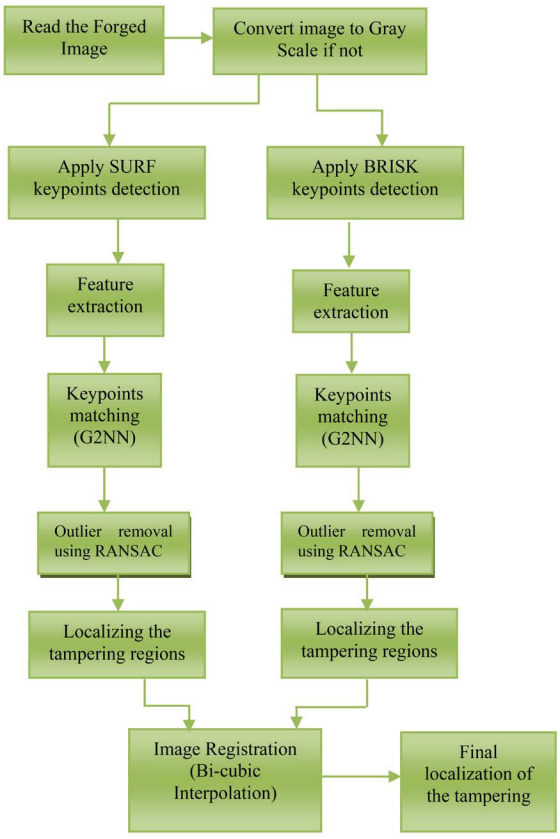

Figure 2. Flow-chart of the proposed forgery detection algorithm.

3.1.1. SURF Keypoints Detection

SURF algorithm is also computationally faster compared to other feature keypoints extraction methods. The first step is to convert the forged image into grayscale image as SURF algorithm runs over grayscale images. Commonly, classic SURF algorithm has two major steps:

1) Keypoints detection and description.

2) Keypoints Matching.

To detect the keypoints, SURF uses:

- an approximation to the Hessian matrix along with box filters,
- integral images,
- and non-maximum suppression.

On the descriptor side:

- Given a set of keypoints, each one is described by using Haar Wavelet coefficients on vertical and horizontal directions from a circular region around them.
- The coefficient values are weighted by a Gaussian window.
- And compose the final 64-d descriptor for a specific keypoint.

1) Keypoints Detector

The detector is based on Hessian matrix. An integral Image decreases the computation speed increases the performance and reduces the time complexity [10]. An Integral image of an image I at a given point $X=(x,y)$ is described as the summation of all pixels' intensities in an image I formed by the point X from the origin as in (1).

$$I_{\Sigma}(X)=\sum_{i=0}^{x}\sum_{j=0}^{y}I(i,j) \tag{1}$$

KeyPoint Detection requires scale space building for the keypoints' extraction. To detect the keypoints' locations, they are where the determinant is maximum. In SURF algorithm, LOG (Laplacian of Gaussian) is estimated by a box filter. Convolution is applied to the image with a box filter of varying size for constructing the scale space. After building the scale space, the Hessian matrix's determinant is calculated for detecting the ultimate point. If the determinant is positive that means, both the Eigenvalues are of the same sign either both are negative or both are positive. In a situation of the positive result, points will be taken as an extreme; otherwise, it will be discarded. The Hessian matrix is defined as $H(x,\sigma)$ for a given point $X=(x,y)$ in an image I as follows:

$$H(x,\sigma)=\begin{bmatrix}L_{xx}(x,\sigma) & L_{xy}(x,\sigma)\\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma)\end{bmatrix} \tag{2}$$

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 $L_{yy}(x,\sigma)$. The 9 × 9 box filters are approximation of the Gaussian and $\sigma=1.2$ represents the lowest scale (*i.e.*, the highest spatial resolution) for computing the keypoint feature vector. The approximate determinant of the Hessian matrix is calculated by:

$$|H| = D_{xx}D_{yy} - \left(0.9D_{xy}\right)^2 \quad (3)$$

where: 0.9 represents the weights applied to the rectangular regions are simple for computational efficiency, D_{xx}, D_{xy}, and D_{yy} are the second order Gaussian derivatives approximations in *x*, *xy* and *y* direction respectively. The approximated determinant of the Hessian represents the keypoint in the image at the specified location.

2) Keypoints Descriptor

SURF keypoints descriptors are built after finding the keypoints. This is done using Haar-wavelet coefficients in the x and y directions, at the scale the key point was detected. The dominant orientation is estimated by summing all of the responses in a sliding window. Next, the region is divided into smaller sub-regions and some features are computed (weighted Haar wavelet responses in both directions, sum of the absolute values of the responses). After assembling the keypoints and descriptors, we calculate likeness among them. We specify that a keypoint has one matching only over the image. To assure this, we use the Generalized 2 Nearest Neighbor policy among the descriptors of each keypoint to identify similar areas in the forged image.

The idea of G2NN is that if the ratio of $\frac{d_i}{d_{i+1}}$ is less than a threshold T and k (where $1 \le k \prec n$) is the value in which the procedure stops, each keypoint in correspondence to a distance in $\{d_1, d_2, \cdots, d_k\}$ is considered as a match for the inspected keypoint. Our approach uses the Hamming Distance between descriptors to evaluate similarities. To minimize the false positives number, we apply one more threshold over the distances, banning close keypoints to be incorrectly matched.

If the distance length between two closed keypoints is very small, these matched keypoints probably is a mismatch. In this paper if the distance between two keypoints is less than threshold $Dis_{\min}$, they will be deleted. Next, to identify the prospective cloned areas, hierarchical cluster is executed on locations of the matched keypoints. After clustering, we also apply the RANdom SAmple Consensus algorithm (RANSAC) [16] to delete mismatched points. At the final step, if the number of matching between clusters is greater than three pairs, the image is considered tampered. Then the copied and pasted regions are localized by joining the matched keypoints using line.

3.1.2. BRISK Keypoints Detection

BRISK algorithm is dramatically the least computational complication. This algorithm is faster than SURF. The BRISK keypoint feature vector is built as an assembly of bit-string vector. This binary keypoint vector is composed of three parts:

a) A sampling pattern: where to sample neighborhoods in the region around the keypoint.

b) Orientation compensation: a procedure to gauge the orientation of the keypoint and rotate it to compensate for rotation changes.

c) Sampling pairs: which pairs are used to compare when constructing the final keypoints' vector.

1) Computing Orientation

For computing the orientation of the keypoint, BRISK uses local gradients between the sampling pairs which are defined by as in (4):

$$g(X,Y)=(X-Y)\frac{I'(x)-I'(y)}{\|X-Y\|^2} \tag{4}$$

where: $g(X,Y)$ is the local gradient between the sampling pair (X, Y), I' is the smoothed intensity value.

By using two thresholds $\delta_{\min}$ and $\delta_{\max}$, the pair points are divided into two groups S (*short*) *and* L (*long*). Long pairs are used in BRISK to determine orientation and short pairs are used for the intensity comparisons that build the descriptor as in Equation (5):

$$S=\left\{(X,Y)\middle|\|X-Y\|<\delta_{\max}\right\} \text{ and } L=\left\{(X,Y)\middle|\|X-Y\|>\delta_{\min}\right\} \tag{5}$$

To compute orientation, summing up all the local gradients between all the long pairs only and take $\arctan\frac{g_y}{g_x}$ —the arctangent of the y component of the gradient divided by the x component of the gradient. This gives the angle of the keypoint. BRISK only uses long pairs for computing orientation based on the assumption that local gradients eliminate each other thus, it is unnecessary in the global gradient determination.

2) Keypoints Vector Construction

Constructing the descriptor is done by performing intensity comparisons. BRISK takes the set of short pairs, rotate the pairs by the orientation computed earlier and makes comparisons of the form in (6):

$$b=\begin{cases}1 & \text{if } I'\left(Y^{\alpha}\right)\succ I'\left(X^{\alpha}\right)\\ 0 & \text{otherwise}\end{cases} \tag{6}$$

$\forall\left(X^{\alpha},Y^{\alpha}\right)\in S$. The result is a bit vector of length 512 keypoints.

Meaning that for each short pair it takes the smoothed intensity of the sampling points and checked whether the smoothed intensity of the first point in the pair is larger than that of the second point. If it does, then it writes 1 in the congruous bit of the descriptor and otherwise it will be 0. Remember that BRISK uses only the short pairs for building the descriptor.

The binary features resulted from BRISK are matched for similarity using *G2NN* search. Hamming distance is used to find the nearest neighbor. Hamming distance is the difference of the number of bits in two compared bit strings. Similarly, as done with SURF keypoints feature, RANSAC is also used to remove outliers or inconsistent matches. It is usually used to minimize the false detection rate and eliminate the outlier keypoints.

3.2. The Refine Detection Stage

Image Registration is the determination of a geometrical transformation that

aligns pixels in one view of an area with corresponding pixels in another view of that area. The inputs of registration are the two views to be registered; the output is a geometrical transformation, which is merely a mathematical mapping from pixels in one view to pixels in the second. To the extent that corresponding pixels are mapped together, the registration is successful. This mathematical mapping is done here in this paper by using the bi-cubic interpolation between the corresponding pixels.

Bi-cubic mapping performs a better job of preserving fine details and is usually used in commercial image editing programs e.g. adobe Photoshop [17]. Using bi-cubic mapping gives more smooth results and fewer artifacts. It takes into account the nearest neighbor 16 pixels (4 × 4) of a specific pixel. It can be calculated as in (7):

$$I(x,y)=\sum_{i=0}^{3}\sum_{j=0}^{3}a_{ij}x^{i}y^{j} \tag{7}$$

where: a_{ij} is the interpolation coefficient. x^{i} is the extracted keypoint at position i by using SURF, and similarly y^{j} is the extracted keypoint at position j by using BRISK. $I(x,y)$ is consisting of multiplying the 16 interpolation coefficients by the dot product of x^{i} and y^{j}.

To summarize the steps of bi-cubic mapping for a certain position:

1) Identify the 16th neighbors of this position in vector of BRISK and the corresponding one in vector of SURF.

2) Determine the value of the 16th interpolation coefficients.

3) Cross product the value of each neighbor in BRISK by the corresponding one in SURF and then multiply the result by the corresponding value of the interpolation coefficient.

4) Repeat step 3 over the 16th neighbors.

5) Sum the resulting value over the 16th neighbor to get the bi-cubic mapping.

4. Experimental Results

In this section, we extensively discuss the experimental environment. The proposed technique use an amalgamation of SURF and BRISK as a feature extraction techniques and bi-cubic interpolation to merge the results' outcome from the both features, to increase the forgery detection accuracy. Four different standard well known dataset are used to run the experiment to check the accuracy and efficiency of the proposed technique. This will efficiently prove the validation of the proposed technique. The proposed technique parameters are set optimally based on previous best practices. Performance evaluation and numerical analysis of the proposed forgery detection technique are examined comparatively to one of the previously published technique [12], which is based as well on SURF and BRISK feature extraction techniques.

4.1. Experimental Setup

To experience digital forgery detection technique, a dataset comprising different

types of forgery is required. In this experimental study, we have used realistic datasets to evaluate the performance of the proposed technique, the CASIA tampered image detection evaluation database V2.0 (CASIA, 2010) [18] is one of them. The datasets include samples of copy-move and copy-paste digital forgeries applied on images of varied sizes. The image region selected for duplication can be transformed before copying them by applying scaling, rotation, reflection, or distortion. The duplicated area varies in size. An example of forged image and the original image from the CASIA dataset is shown in **Figure 3**. The algorithm is coded in MATLAB R2014 on a machine equipped with Intel i5 2.00 GHz processor with 3GB DDR3 RAM.

4.2. Evaluation Metrics

For evaluating all the techniques, we chose the three following metrics, in accordance to the ones used in the 1st IEEE Intl. Image Forensics Challenge in 2013 (IFC):

- **True Positive Rate (TPR)**: indicates the percentage of correctly located reduplicated regions. It is calculated as in (8):

$$\mathrm{TPR} = \frac{|TP|}{|R_{clone}|} \tag{8}$$

where $|TP|$ (True Positive) represents the number of pixels correctly classified as cloned in the detection map, and $|R_{clone}|$ represents the number of real cloned pixels in the reference map.

- **False Positive Rate (FPR)**: indicates the percentage of incorrectly located reduplicated regions. It is calculated as in (9):

$$\mathrm{FPR} = \frac{|FP|}{|R_{clone}|} \tag{9}$$

where $|FP|$ (False Positive) represents the number of pixels wrongly classified as copied in the detection map, and $|R_{clone}|$ represents the number of pixels, in the reference map, that do not belong to the copied regions.

- **Accuracy (ACC)**: gives the total quality of detection based on True Positive Rate and True Negative Rate, which indicates the percentage of correctly located non-cloned regions. It is calculated as in (10):

$$\mathrm{ACC} = \frac{\mathrm{TPR} + (1 - \mathrm{FPR})}{2} \tag{10}$$

4.3. Performance Evaluation and Its Analysis

The performance of the proposed technique is compared with another technique using different benchmark datasets mentioned in the above sections. Specifically; the technique proposed in [12]. This technique is also based on the hybridization between SURF and BRISK. The technique is tested using correct detection a ratio which is ratio of valid keypoints to total matched keypoints. The proposed technique is divided into three sections:

(a) Original Image (b) Forged Image

Figure 3. A sample of images and the ground truth in the CASIA dataset [18].

1) Extracting SURF keypoints;

2) Extract BRISK keypoints;

3) Matching descriptors to locate the forged regions using image registration by bi-cubic interpolation.

Results show that the SURF descriptors are invariant to geometrical transformations. It has been also observed that it is quite suited in detecting the image region duplication consisting of additive noise and blurring.

The time taken by the proposed algorithm is much comparing to the technique in [12], because our supposed technique using more computations:

1) In the detection stage by:

- Using G2NN instead of KNN.
- The execution of SURF and BRISK individually and in a parallel way instead of using SURF as a prior to BRISK.

2) In the refine stage by using bi-cubic interpolation, and there is no refine stage in technique proposed in [12].

The time comparison is provided in **Table 1** for descriptor extraction. The technique is evaluated for stability by correct detection ratio, which is a ratio of the keypoints in the forged region to the total keypoints detected.

To analyze the performance of evaluating copy-move forgery detection algorithms at image level, we use the following error measures provided to the ones previously mentioned above in Equations (8) (9) and (10). It concentrates on whether the truth that an image has been faked or not to be detected. So; both the measures of precision and recall should be calculated to verify the validity of the techniques. Precision and recall can be calculated as in 11 and 12 respectively:

$$\text{Precision} = \frac{T_p}{T_p + F_p} \tag{11}$$

$$\text{Recall} = \frac{T_p}{T_p + F_N} \tag{12}$$

where: T_P—The number of accurately detected forged images.

Table 1. Comparison of average detection with existing technique.

Technique	Average Detection Time per Seconds
Existing Technique in [12]	5.4
Proposed Technique	8.2

F_P—The number of images that have been mistakenly detected as forged.

F_N—Incorrectly missed forgery images.

Precision denotes the probability a detected tampered image being a truly tampered image; while Recall shows the probability of a truly tampered image being detected as tampered. Recall is usually called true positive rate as well. Score as a comprehensive measure which merges precision and recall in one measure.

$$\text{Score} = \frac{2 * P * R}{P + R} \tag{13}$$

where P represents precision and R represents recall.

The experiment is carried out on image datasets with different size images. **Figure 4** and **Figure 5** show the detection results for different kinds of processing operations inclusive rotation and scaling. The time taken to detect forgery is not directly dependent upon the image size; actually it depends upon the duplicated area size. The number of keypoints generated and the corresponding descriptors processed are proportional to the duplicated region and brightness variations. **Table 2** and **Table 3** show high stability of the method in terms of correct detection ratio.

Technique in [12] used SURF as a prior to BRISK which means that if there are any interesting keypoint lost in SURF detection will be as well in applying BRISK to the image resultant from the SURF feature extraction. Thus; the efficiency of technique in [12] is not the quite perfect because of the missing of some keypoints and the SURF extraction stage and cannot be considered again in BRISK extraction as it is already doesn't include in the image passed to BRISK. In our proposed technique, we aimed to solve this challenge faced the authors in [12]. We work on both features extraction in parallel way to fully utilizing the keypoints extracted from the both features. By using the interpolation between the two extracted feature, the most interesting common keypoints are resulted which enrich the efficiency of the forgery detection.

5. Conclusion and Future Work

In this paper, we performed a deep analysis of the copy-move forgery detection problem by first presenting its main challenges, as well as several ideas (in the literature) that increased our understanding about the characteristics of the problem. The main aspect we have found out to be incipient in other methods has been regarding to the combination of post-processing operations, although there was still much to be improved when tackling such operations alone. A

Table 2. Comparison of precision, recall and score for copy-move attack.

Technique	Precision	Recall	Score
Existing Technique in [12]	91.49%	89.58%	90.53%
Proposed technique	94.03%	92.31%	93.01%

Table 3. Comparison of TPR, FPR and ACC for copy-move attack.

Technique	TPR	FPR	ACC
Existing Technique in [12]	93.63%	8.99%	92.32%
Proposed technique	97.4%	6.74%	95.33%

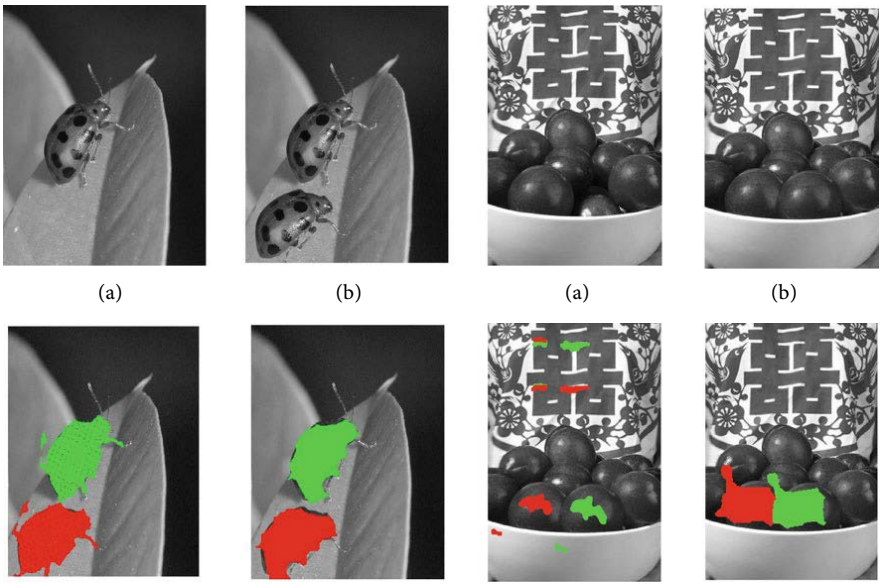

Figure 4. Detection of image forgery, (a) Original image, (b) Forged image, (c) Detected forged region using [12] and (d) Detected region using the proposed technique.

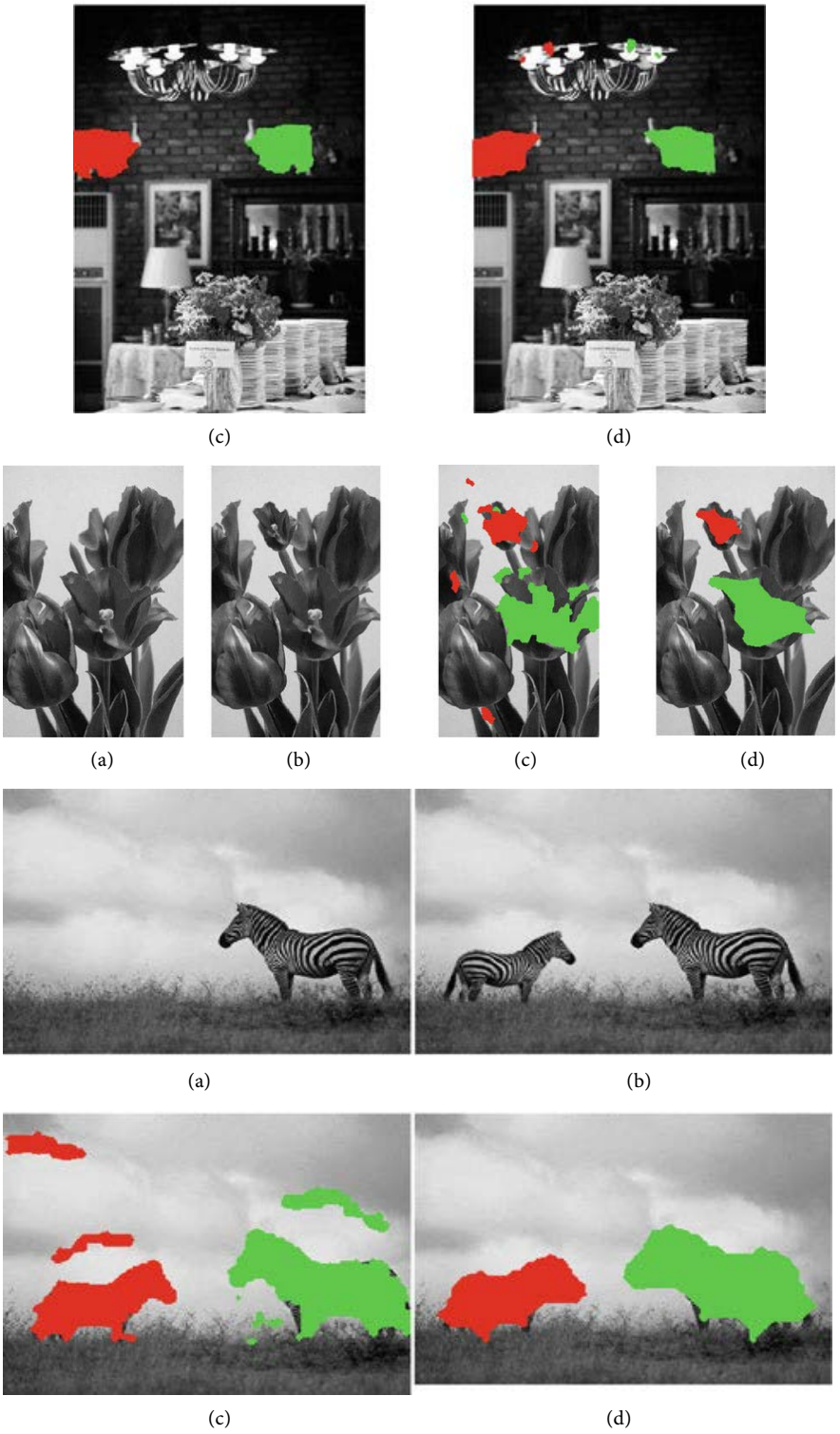

Figure 5. (a) Original image, (b) Forged image, (c) Detection result using technique in [12], and (d) Detection result using the proposed technique.

copy-move forgery detection technique is provided based on keypoints extraction and matching. The areas of copy-move forgery are detected basically by comparing the key points extracted in the image. It is so effective to affine transformations

such as rotation and scaling as well as other post-processing operations like JPEG compression and Gaussian noise addition. Compared with other key point-based techniques published, the proposed technique almost requires two steps, namely the parallel execution of SURF and BRISK, and the bi-cubic interpolation estimation refinement. SURF has a minimal feature keypoint descriptor dimensional length. Thus, matching process applied on SURF keypoints is faster and decreases the computation speed as well. The Haar wavelets that are used for feature descriptors computation from each keypoint result in that these descriptors are robust to illumination changes. The experimental results demonstrate the efficacy the proposed technique has in detecting the flat duplication regions with various post-processing operations within a reasonable detection time.

Certainly, there is no gold bullet to solve completely the whole problems and we are aware that the proposed technique is just a step toward solving the cloning detection problem. However, we believe our technique presents several contributions that will provide the literature with new ways to cope with this challenging problem. Finally, with the low false-positive rates found and high reliability regardless the testing scenario (low deviations across different testing conditions), we also think our contribution may be very useful in a real-world forensics scenario, providing an investigator with a set of suspect cloning regions to be visually checked in the image, as one of the prior steps in determining its authenticity.

The proposed technique overcame the problem of false detection comparing to the technique proposed in [12]. The proposed technique gives a high accuracy of detection because it is fully utilizing the keypoints extracted from both SURF and BRISK, additionally it combined them using the bi-cubic interpolation which enriched the score of detection and decreased the false detection rate. While, this process enhanced the accuracy but it was a more time consuming than the technique in [12]. The proposed technique overcame as well the problem of smooth and flat regions detections as indicated in experimental results and **Figure 4** and **Figure 5**.

In the future, we will try to improve the detection speed of the proposed technique by using parallel programming. Additionally, we can enhance the detection performance in handling very small and very smoothed forged regions using a different matching method in both SURF and BRISK.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] GIMP. https://www.gimp.org

[2] NIK Collection. https://nikcollection.dxo.com/download

[3] Kaur, R. and Kaur, A. (2016) A Review of Copy-Move Forgery Detection. *IRASCT*

International Journal of Computer Science and Information Technology & Security, **6**, 249-253.

[4] Bhalla, C. and Gupta, S. (2016) A Review on Splicing Image Forgery Detection Techniques. *IRACST International Journal of Computer Science and Information Technology & Security*, **6**, 262-269.

[5] Kaur, H., Saxena, J. and Singh, S. (2015) Simulative Comparison of Copy-Move Forgery Detection Methods for Digital Images. *The International Journal of Electronics, Electrical & Computational*, **4**, 62-66. https://doi.org/10.17577/IJERTV4IS061110

[6] Mohmood, T. (2015) A Survey on Block Based Copy-Move Image Forgery Detection Techniques. *Proceeding of the International Conference on Emerging Technologies*, Peshawar, 19-20 December 2015, 1-6.

[7] Mahmood, T., Mehmood, Z., Shah, M. and Saba, T. (2018) A Robust Technique for Copy-Move Forgery Detection and Localization in Digital Images via Stationary Wavelet and Discrete Cosine Transform. *Journal of Visual Communication and Image Representation*, **53**, 202-214. https://doi.org/10.1016/j.jvcir.2018.03.015

[8] Tralic, D., Zupancic, I., Grgic, S. and Grgic, M. (2013) CoMoFoD—New Database for Copy-Move Forgery Detection. *The Proceeding of the ELMAR*, Zadar, 10-12 September 2014, 49-54.

[9] Shi, W.C., Zhao, F., Qin, B., *et al*. (2016) Improving Image Copy-Move Forgery Detection with Particle Swarm Optimization Techniques. *Journal of China Communication*, **13**, 139-149. https://doi.org/10.1109/CC.2016.7405711

[10] Bay, H., Ess, A., Tuytelaars, T. and Gool, L.V. (2008) Speeded-Up Robust Features (SURF). *Journal of Computer Vision and Image Understanding*, **10**, 346-359. https://doi.org/10.1016/j.cviu.2007.09.014

[11] Leutenegger, S. and Chli, M. (2011) BRISK: Binary Robust Invariant Scalable Keypoints. *Proceeding of the IEEE International Conference on Computer Vision*, Barcelona, 6-13 November 2011, 2548-2555. https://doi.org/10.1109/ICCV.2011.6126542

[12] Kumar, S. and Desai, J.V. (2015) A Fast Keypoint Hybrid Method for Copy Move Forgery Detection. *International Journal of Computing and Digital Systems,* **4**, 91-99. https://doi.org/10.12785/ijcds/040203

[13] Ojeniyi, J.A. (2018) Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques. *International Journal of Image, Graphics and Signal Processing*, **10**, 22-30. https://doi.org/10.5815/ijigsp.2018.04.03

[14] Antony, N. and Devassy, B.R. (2018) Copy-Move Image Forgery Detection Using Adaptive Over-Segmentation and Brute-Force Matching. *International Journal of Advanced Research Trends in Engineering and Technology*, **5**, 25-30.

[15] Devi, P. and Deswal, S. (2018) Clustering Based Feature Extraction for Image Forgery Detection. *International Journal of Computer Sciences and Engineering*, **6**, 22-27. https://doi.org/10.26438/ijcse/v6i7.2227

[16] Fischler, M.A. and Bolles, R.C. (1981) Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography. *The Journal of Communications of the ACM*, **24**, 381-395. https://doi.org/10.1145/358669.358692

[17] Dhivya, B. and Sundaresan, M. (2016) Performance Analysis of Interpolation Methods for Improving Sub-Image Content-Based Retrieval. *Proceeding of* 3*rd International Conference on Computing for Sustainable Global Development*, New Del-

hi, 16-18 March 2016, 3909-3912.

[18] CASIA (2010) Image Tampering Detection Evaluation Database, Ver. 2.0. http://forensics.idealtest.org