Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal

Aya Hegazi *, Ahmed Taha, Mazen M. Selim

Faculty of Computers & Informatics, Benha University, Egypt

ARTICLE INFO

Article history:
Received 11 April 2019
Revised 17 July 2019
Accepted 21 July 2019
Available online xxxx

Keywords:
Copy-move detection
Image forensics
Keypoint-based methods
Multiple-copied matching
DBSCAN
GORE

ABSTRACT

Copy-move image forgery detection has become a significant research subject in multimedia forensics and security due to its widespread use and its hard detection. In this type of image forging, a region of the image is copied and pasted elsewhere in the same image. Keypoint-based forgery detection approaches use local visual features to identify the duplicated regions. The performance of keypoint-based methods degrades in those cases when the duplicated regions are near to each other and when handling highly textured area. The clustering algorithm that mostly used in keypoint- based methods suffer from high complexity. In this paper, an improved approach for keypoint- based copy-move forgery detection is proposed. The proposed method is based on density-based clustering and Guaranteed Outlier Removal algorithm. Experimental results carried out on various benchmark datasets exhibit that the proposed method surpasses other similar state-of-the-art techniques under different challenging conditions, such as geometric attacks, post-processing attacks, and multiple cloning.
© 2019 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Verifying integrity and authenticity of digital images is still an operational challenge. In the last decade, several digital image forensic techniques have been developed (Lin et al., 2018). Research has focused on passive (or blind) image forensics (Al-Qershi and Khoo, 2013; Bakiah et al., 2016; Cozzolino et al., 2015). It is aimed to determine authenticity of digital images without any prior information about the image as opposed to watermarking techniques (Christlein et al., 2012; Bakiah et al., 2016). In blind image forensics, many types of forgery can take place. Copy-move (or cloning) forgery detection is one of the most common subtopics in forgery research (Christlein et al., 2012; Li et al., 2015; Bakiah et al., 2016). In this type, at least one region is copied and pasted somewhere else in the same image. Suppressing the truth or hiding specific information in the image is the main purpose of copy-move forgery. A typical example of copy-move forgery is illustrated in Fig. 1. Fig. 1(a) and (b) are the original images, while Fig. 1(c) and (d) are fake images. In Fig. 1(c) part of textured wall was duplicated and placed over the base of the wall below. While in Fig. 1(d), trees are used as a manipulated area to hide the building. As the source and copied regions from the same image, they share the same properties such as color temperature, illumination effect, and texture. To mislead the human eye, various types of post-processing operation such as JPEG compression and noise addition or affine transformations such as scaling, rotation, and translation are applied to the copied region. Tracing these manipulations in the image is usually hard for ordinary people. Copy- move forgery can be detected by analyzing these similar image region pairs based on the correlation between them.

Generally, block-based and keypoint-based are the two main categories of Copy-Move Forgery Detection (CMFD) methods (Christlein et al., 2012; Bakiah et al., 2016). The pipeline introduced in (Christlein et al., 2012) is commonly followed by all CMFD methods in the literature as shown in Fig. 2. This pipeline based on three main steps: Feature extraction, matching and post-processing. These operations can be achieved either densely for each pixel of the image as in block-based methods or sparsely for some selected keypoints as in keypoint-based methods. For both cases, the image is possibly pre-processed depending on the application. The image is converted into suitable color space, mostly into grayscale. In the feature extraction stage, image is split into square or circle blocks (or regions) with fixed dimensions in block-based methods. For each block, compute a feature vector. Matching is accomplished

* Corresponding author.
E-mail address: aya.moghawry@fci.bu.edu.eg (A. Hegazi).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2019.07.007
1319-1578/© 2019 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

Fig. 1. Example of image with a typical copy-move forgery. (a), (b) The original images. (c), (d) The tampered images.

Fig. 2. Common processing pipeline for copy-move forgery detection.

between Similar feature vectors. Unlike block-based, Keypoint-based methods extract the distinctive local features from the image. Afterward, a similar feature descriptors are matched. Then to reduce the probability of false matches, the image is filtered. Finally, post-processing is done by analyzing filtered result and preserving matches with common behavior for forgery detection and localization. It must be considered that the set of matches in both source and target blocks (or keypoints) are spatially close to each other. Moreover, matches that created from the identical copy-move behavior should demonstrate similar amounts of geometric transformation such as translation, rotation, and scaling (Christlein et al., 2012).

The two key issues in copy-move forgery detection methods are accuracy and efficiency. They must achieve fewer errors, time and memory requirements under various image sizes and distortions. The computation time relies on both the feature set complexity and on the feature vector size (Christlein et al., 2012). The feature size result from block-based methods can cause very high memory use especially for large images. Keypoint-based methods overpass in space and time complexity. The reason is that the number of extracted keypoints is typically smaller than the number of image blocks. This gives a very light weight of the whole subsequent processing. Therefore, carrying out these two issues are profoundly challenged. These observations are at the core of our work presented here. An improved technique for copy-move forgery detection is proposed. It successfully reduces false alarms with more accurate results.

2. Related work

As discussed earlier, there are two methods for detecting copy-move forgery: block-based and keypoint-based. Block-based methods are also known as dense field methods because all the pixels go through the phase of feature extraction. Unfortunately, block-based methods are known to result in high computational complexity because all features are searched exhaustively in the matching phase. In the literature, various enhancements techniques based on block-based approaches can be found such as: Discrete Cosine Transform (DCT), Fourier-Mellin Transform (FMT), Discrete Wavelet Transform (DWT), Histogram of Orientation Gradient (HOG), Signal Value Decomposition (SVD), and Zernike Moment. They have been introduced to further improve the performance of CMFD techniques (Christlein et al., 2012; Al-Qershi and Khoo, 2013; Qureshi and Deriche, 2015). Nevertheless, DCT and ZERNIKE moment features recorded the best results among block-based methods (Christlein et al., 2012). Of all block-based methods, DCT is one of the most vastly used methods in CMFD (Bakiah et al., 2016). The DCT coefficients are used as features to detect the duplicated regions. Robustness against JPEG compression and noise addition is one of the most important strengths of DCT-based approaches. However, when applying high levels of post-processing operations, such as blurring and geometric transformations, DCT-based approaches fail to detect copy-move forgery (Asghar et al., 2017; Christlein et al., 2012). Detection based on DCT was first proposed by (Fridrich et al., 2003). Detection method presented by (Cozzolino et al., 2015) attempted to reduce the complexity of the matching phase by utilizing PatchMatch algorithm. Nevertheless, even for small image size, the computational complexity remains nowhere near-real time. (Alkawaz et al., 2018) studied the effect of various block size based on DCT for CMFD. Their method does not handle the post-processing operations. In addition, authors (Bi and Pun, 2017), suggested a fast-reflective offset guided searching method. It is based on an iterative process to optimize the feature matching phase for CMFD. One limitation of this method is its failure to detect forgery when large intensity value of noise addition is applied. Recently, (Hayat and Qazi, 2017) suggested a method based on DCT and DWT. In this method, the processed image is subjected to DWT to get the approximated lowest energy sub-band. Then, DCT is applied to each individual block of DWT sub-band. They used correlation coefficients for blocks comparison to find the duplicated regions. Their method suffers from a high computational load and they do not consider any post-processing operations. From the previous concerns, it has proven that applying block-based methods is not suitable for real-time implementations and they usually result in high false positives.

On the other hand, keypoint-based methods try to address these issues for both computation complexity and robustness to post-processing operations. Unlike block-based methods, they rely on identifying high entropy regions (i.e. keypoints) from the image. Consequently, they give only few feature vectors, which lead to lower computational complexity and smaller false positives rate. The most popular and reliable keypoint features technique in CMFD is Scale Invariant Feature Transform (SIFT) (Bakiah et al., 2016). The generalized 2-nearest neighbor (G2NN) procedure for SIFT descriptor matching was first introduced in (Amerini et al., 2011) to detect multiple copy-move forgeries. Their method is based on SIFT and Agglomerative Hierarchical Clustering (AHC). Later, they improved their work in (Amerini et al., 2013) by introducing a method based on J-linkage algorithm for clustering. To enhance matching performance and obtain better feature coverage, authors in (Yu et al., 2016) introduced two-stage feature detection method based on Hue Histogram (HH) and Multi-support Order-based Gradient Histogram (MROGH) descriptor. Moreover, a CMFD based on Multi-Level Dense Descriptor (MLDD) and a hierarchical feature matching is presented in (Bi et al., 2016). The MLDD extraction method uses multiple levels to extract the dense features. After that hierarchical feature matching is ap- plied to detect forged regions in the input image. (Wang et al., 2016) introduced a detection method for small smooth regions based on superpixel segmentation and Speed up Robust Feature (SURF). Although this method recorded a good detection accuracy, it cannot be used in real-time applications due to its high computational complexity. In (Jin and Wan, 2017), presented SIFT-based method using non-maximum value suppression and optimized J-Linkage. Another segmentation-based method presented in (Bi et al., 2018) where

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University –
Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

the host image is segmented into non-overlapping irregular patches by applying Simple Linear Iterative Clustering (SLIC) algorithm. Then SIFT is utilized to extract feature points from all patches to create the multi-scale features. For the matching phase, the adaptive patch-matching algorithm is used. A SIFT-based method introduced by (Abdel-Basset et al., 2018) applied clustering at two-level: in the spatial domain and in the frequency domain. Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm is used in spatial domain followed by Random Sample Consensus (RANSAC) algorithm in the frequency domain.

To sum up, keypoint-based methods generally and SIFT-based techniques specifically have proved its strength and effectiveness compared to block-based methods. Even though these methods still have various limitations. Most of the existing keypoint-based methods use clustering or segmentation, which profoundly affected all subsequent processing in term of time and space complexity. Moreover, they yield a high false positive rate especially when handling highly textured area.

3. Proposed method

In this paper, a keypoint-based copy-move forgery detection method is proposed. It effectively reduces the false positive rate and improves time and space complexity. The contributions of the proposed method include: 1) by utilizing the (DBSCAN) clustering algorithm, the forged patch can be detected more accurately while reducing time and space complexity. 2) the guaranteed Outlier Removal (GORE) algorithm is employed with RANSAC algorithm to reduce the false matches more effectively. It follows the framework suggested in (Christlein et al., 2012). Fig. 3 illustrates the framework of the proposed method. The details about each phase is illustrated in the following subsections: image preprocessing in Section 3.1, in Section 3.2, features and their descriptors are extracted from the image using SIFT and then matched. Section 3.3 introduces a density-based clustering algorithm and compares it with AHC. Section 3.4 presents a two-level outlier removal and estimate affine transformation.

3.1. Image preprocessing using CLAHE

Keypoint-based methods are known to lack the ability to identify highly identical features or smooth regions. To improve features detection in smooth regions in the proposed method, contrast-limited adaptive histogram equalization (CLAHE) algorithm by (Sia et al., 2013) is used. CLAHE results in less noise and it resists against brightness saturation that commonly results from histogram equalization (Kumar and Sharma, 2008). CLAHE is a variant of adaptive histogram equalization used for low-contrast image enhancement. It reduces the noise amplification problem by introducing a contrast-clipping limit. In CLAHE algorithm, an image is divided into overlapping regions that are called tiles or blocks and for each tile histogram, equalization is applied. Then, each tile's histogram is clipped by a clip limit that relies on the normalization of the histogram and the size of the neighborhood region (Ma et al., 2017). After that, the Cumulative Distribution Function (CDF) such as Gaussian, Poisson or Rayleigh is computed. Tile size and clip limit are two key parameters of CLAHE, which mainly control the enhanced image quality. In our work, clip limit and tile size are set to 0.01 and (4×4) respectively. Rayleigh distribution is the most commonly used histogram clips (Ma et al., 2017). The Rayleigh distribution function is given by:

$$y(i) = y_{min} + \sqrt{2(\alpha^2)\ln\left(1 - \frac{1}{1 - p(i)}\right)} \quad (1)$$

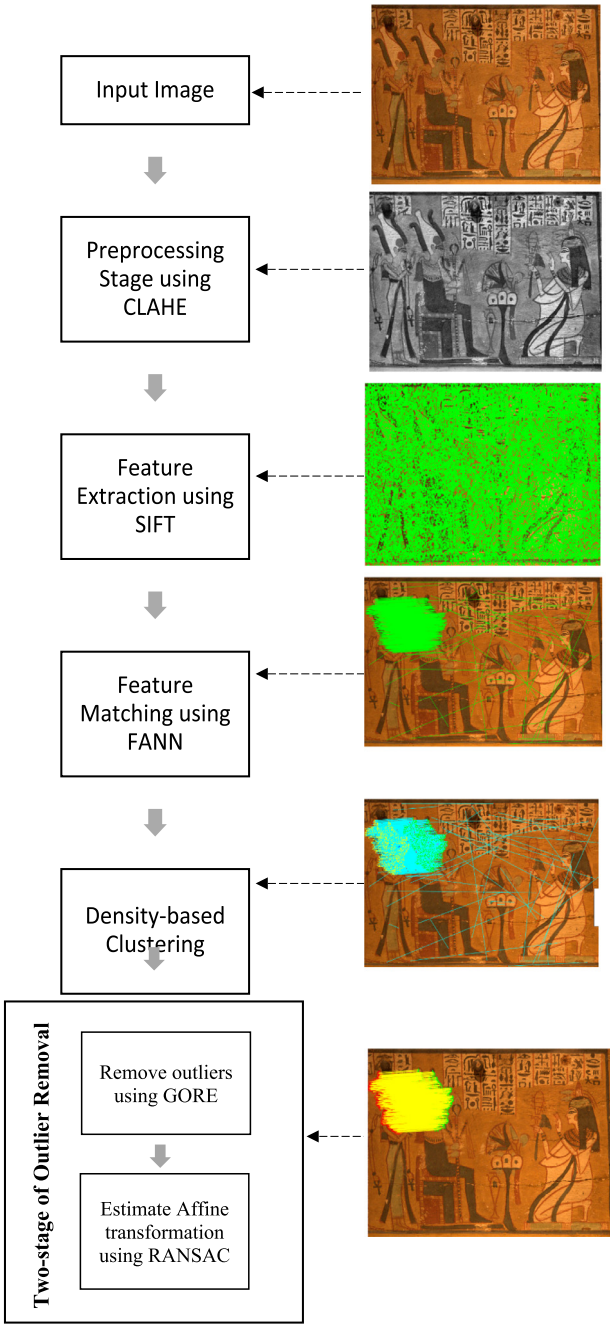

Fig. 3. The Framework of the proposed copy-move forgery detection method.

where, $y_{min}$is the lower bound of the pixel value, α is a scaling parameter of Rayleigh distribution, and $p(i)$ is cumulative probability which is provided to create the transfer function. As the value of α goes higher, the more significant contrast enhancement in the image, at the same time, increases saturation value and amplification of noise levels.

3.2. Keypoint extraction and matching

The proposed method extract keypoints from pre-processed image using Scale Invariant Feature Transform introduced by (Lowe, 2004). SIFT features are invariant to image scale and rotation. It provides a robust matching across the essential range of affine distortion, noise addition, illumination change, and different 3D viewpoints (Lowe, 2004). Compared to other keypoint extrac-

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University –
Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

tion algorithms such as Speeded Up Robust Features (SURF), Binary Robust Invariant Scalable Keypoints (BRISK) and rotated BRIEF (ORB), SIFT is proved to be the most accurate and stable feature detector and descriptor for scale, rotation and, affine variations (Khan and Saleem, 2018). The SIFT algorithm can be summarized shortly as the following: (i) Scale-space peak selection, (ii) Keypoint localization, (iii) Orientation assignment, and, (iv) Keypoint descriptor. To detect the local interest point (keypoint), scale-space is constructed using a difference-of-Gaussian function. Keypoint that is stable local extrema in scale space is found. From a local pixel area around the detected point, the feature vector for each of them is computed. After keypoint's location, scale, and orientation assignments are determined, the local feature descriptor is computed at each keypoint depending on a patch of its local neighborhood pixels. SIFT features are highly distinctive and represented by a 128-dimensional feature vector. Given a test image I, let the set of extracted keypoints and their descriptors denoted by $\boldsymbol{F} = \{f_1, \cdots., f_n\}$, and $\boldsymbol{D} = \{D_1, \cdots., D_n\}$, respectively.

In the copy-move forgery, SIFT features extracted from copied and the original regions have similar descriptor vectors. Thus, matching these features descriptors is essential to detect and localize forgeries. The most used matching procedure in a keypoint-based method is G2NN that was first introduced by Amerini et al. (2011). G2NN is known for its ability to deal with multiple copies of the same features. However, it lacks the high dimensional space and results in a high false negative rate (Christlein et al., 2010). In the proposed method, an Approximate Nearest Neighbor (ANN) method by (Muja and Lowe, 2009) is used for matching. Fast ANN (FANN) provides fast medium and large-scale nearest neighbor search in high dimensional data points. Moreover, it can handle multiple copy-move forgeries. It utilizes randomized k-dimensional trees (kd-trees) for a fast neighbor search (Muja and Lowe, 2009). In general, It has been shown that the use of kd-tree matching causes better results than lexicographical sorting (Christlein et al., 2010). Kd-tree is built using feature descriptor and Best-Bin First (BBF) search heuristic is used to find the k nearest neighbors of each keypoint f_i from all other (n-1) keypoints of the image. Due to the high dimensionality of the feature space, Lowe (2004) considers for a given keypoint, a distance to the first and the second similar keypoints. Specifically, the ratio between the Euclidean distance to the first similar match and the Euclidean distance to the second similar feature point (i.e. 2NN search). This matching ratio should be lower than a predefined threshold T. The matching threshold is set to T = 0.5 to afford a good trade-off between matching accuracy and outliers' ratio.

3.3. Density-based clustering and forgery detection

After obtaining the matching pairs, a clustering algorithm is applied to the keypoint spatial locations to group spatially closed keypoints and detect the cloned regions. The most common clustering algorithm used in CMFD is the AHC (Bakiah et al. 2016). Although the AHC gives best results in some cases and it is not highly sensitive to the choice of distance metric, it has several drawbacks that can affect the accuracy and efficiency of forgery detection. It suffers from low efficiency especially in high dimensional space as it has quadratic time. It can lead to high memory requirements, which makes the algorithm applicable only to medium scale problems. Moreover, it is sensitive to noise and outliers. It is also unable to separate duplicated regions that are close to each other. For these reasons, DBSCAN clustering algorithm (Ester et al., 1996) is applied to solve the above-mentioned drawbacks. DBSCAN is a density-based data clustering algorithm used to separate high-density clusters from low-density clusters. The areas of noise have a lower density than the density in any of the clusters (Ester et al., 1996). It can identify clusters of varying shapes in a dataset containing noise and outliers. Furthermore, it does not require specifying the number of clusters at all, and it does not depend on several experiments and optimizations.

Basically, the DBSCAN algorithm requires only two main parameters: epsilon (eps) and minimum points (MinPts). The first parameter eps is defined as the radius of the neighborhood around a data point. This means that two points are considered neighbors if the distance between them is less than or equal to eps value. The other parameter MinPts is the minimum number of neighbors within radius eps to define a cluster. The concept of core samples is the essential component of the DBSCAN. Core samples are samples that are in areas of high density. Higher or lower values of MinPts and eps respectively denote higher density necessary to form a cluster. There are two types of points in a cluster: core points and border points. Points inside the cluster are core points while points on the cluster's border are border points. Generally, the border point's eps-neighborhood has undoubtedly fewer points than of the core point's eps-neighborhood. The clustering starts with a random data point of matched pairs that has not yet been assigned to a cluster (or visited). Then, the neighbors of this point are extracted using distance eps. The current data point becomes the first point in the new cluster and is labeled as a core point (or a sample) if a sufficient number of MinPts within this neighborhood. Otherwise, the point will be identified as noise (or an outlier). In both cases, this point is marked as visited. The points within distance eps of the core point (i.e. directly reachable) also become part of the same cluster. Then, for each reachable point, the clustering does neighbor jumps and adds them to the cluster. If an outlier is found, it labels it as a border point. This procedure is repeated for all the new points that have been just added to the cluster group until all points are assigned to a cluster or labeled as an outlier. An example of DBSCAN clustering algorithm is illustrated in Fig. 4. In the proposed method DBSCAN parameters are set as follows: eps = 3 and MinPts = 40.

3.4. Two-stage outlier removal and affine transform estimation

The intrinsic self-similarity of natural images such as in structured images usually leads to falsely detected matched pairs. Therefore, to reduce false alarms and putative matches and thus obtain more accurate detection and localization, a two-stage strategy for removing outliers based on GORE (Bustos and Chin, 2015) and RANSAC (Fischler and Bolles, 1981) is introduced. Using this combination will exploit the advantages of both techniques and thus will offer highly robust detection and localization. GORE is an outlier removal technique for rotation search. It is used to safely and efficiently remove outliers. It is based on searching lower and upper bounds iteratively. Authors in (Bustos and Chin, 2015) proved that GORE algorithm reduces a significant amount of the

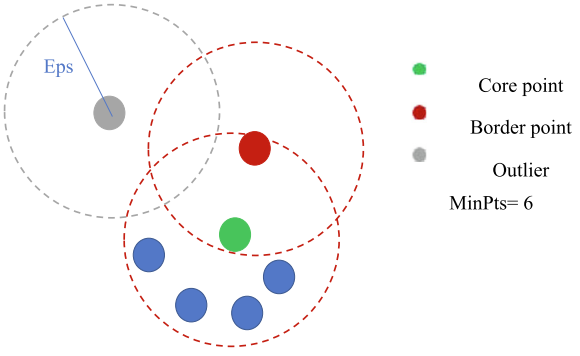

Fig. 4. DBSCAN Clustering.

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University –
Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

outliers and remarkably speeds up the search. When point correspondences with potential outliers are given, it can remove outliers without compromising the global optimality (Bustos and Chin, 2015). In the proposed method, RANSAC algorithm is used to estimate the affine transformation matrix between the original and duplicated regions. Additionally, it filters out mismatches (i.e. outliers). RANSAC algorithm was first presented by Fischler and Bolles. It is a parameter estimation approach which is simple and a powerful. It is utilized to deal with a significant proportion of outliers in the data input. Thus, RANSAC is a popular algorithm used for robust homography estimation (Qureshi and Deriche, 2015; Wang et al., 2016). It is adopted by most of CMFD techniques as in (Amerini et al., 2011; Yang et al., 2017; Yang et al., 2018; Yu et al., 2016; Bi et al., 2016).

At the first stage, after initial clusters have been obtained using DBSCAN clustering, GORE algorithm is applied to each of the matched pairs of clusters. Given two point sets $\mathcal{X} = \{x_i\}_{i=1}^{N}$ and $\mathcal{Y} = \{y_i\}_{i=1}^{N}$, the set of all matched points $\{(x_i, y_i)\}_{i=1}^{N}$ indexed by $\mathcal{H} = \{1, \cdots, N\}$. Each (x_i, y_i) is a pair of matching points. So, given $\mathcal{H}$, GORE iterates over each point match and performs two operations: (i) try to find an improved lower bound $\updownarrow$ (ii) and upper bound f_k to subproblem P_k. Both steps are handled concurrently using an efficient algorithm for upper bound (Bustos and Chin, 2015). Then to reject the current match as an outlier, both values are compared. Therefore, GORE aims to reduce $\mathcal{H}$ to a subset $\mathcal{H}$ of point matches, in a way that any (x_i, y_i) discarded by reducing $\mathcal{H}$ to $\mathcal{H}$ is an actual outlier, i.e., any (x_i, y_i) that is removed does not belong to the globally optimal solution $\mathcal{I}^*$,such that:

$$\mathcal{I}^* \subseteq \mathcal{H} \subseteq \mathcal{H} \tag{2}$$

in which,

$$(x_i, y_i), i \subseteq \mathcal{H}$$

At the second stage, the initial set of filtered keypoints pairs $\mathcal{H}$ from GORE is fed to RANSAC algorithm. It randomly selects at least three spatially adjacent non-collinear pairs from the matched keypoints and estimates the transformation matrix H, such that:

$$X = HX \tag{3}$$

where X and X are the coordinates of corresponding matched pairs in the copying source and pasting the target regions. The transformation matrix can be calculated by means of minimizing the geometric distance $\sum_{i=1}^{n} d(X, HX)$. All the keypoints pairs are then classified either as inliers or outliers according to the following condition:

$$||\widetilde{X} - HX|| \leq \beta \tag{4}$$

For the classification threshold β. This procedure is repeated N_i times. After each iteration, it outputs the estimated transform parameters that lead to the largest number of inliers as a duplicated region. In our experiment, the RANSAC parameters β and N_i are set to 0.03 and 1000, respectively.

Although using RANSAC only can provide us with robust estimation of the transformation matrix and remove mismatches, it is still not accurate enough. Furthermore, some of the detected regions may be just false matches and not holding any of copy-move forged regions. For that, a two-stage outlier removal depending on both GORE and RANSAC algorithms is proposed. Using GORE algorithm at the first stage of outlier removal in our work has remarkably reduced the false positives and improved the forgery detection as clarified in the experimental results.

4. Experimental results

In this section, the results of the proposed CMFD approach are presented. Experimental results have been compared with other state-of-art schemes using two benchmark datasets. All measurements are performed on a desktop computer with Intel Core i5 1.7 GHz CPU and 4 GB RAM memory, running Matlab 2016b.

4.1. Test image database

In this paper, the proposed method is evaluated on two public available datasets: MICC-F220 (Amerini et al., 2011) and image manipulation dataset (Christlein et al., 2012). The MICC-F220 introduced in (Amerini et al., 2011) consisting of images of author's personal collection and images with different contents from the Columbia photographic image repository (Tian-Tsong Ng et al., 2005). It consists of 220 images: 110 tampered images and the other 110 are originals. The resolution of the images ranges from 722×480 to 800×600 pixels and, on the average, the size of the forged region covers 1.2% of the whole image. The forged images have been constructed by choosing a rectangular or square region of an image and copy-pasting it randomly along with the image after assigning various attacks. These attacks are rotation and scaling. Combinations of them have been used to create forged images. In this dataset, no post-processing operations are applied to forged images, such as additive noise or JPEG compression. There are no ground truth images attached in this dataset. The second dataset that was constructed by (Christlein et al., 2012) is a realistic and challenging dataset. Its tampered images were created manually by skilled artists. It consists of 48 original images and 87 copied snippets that are pasted in the same image at different locations to create the forgeries. The copied snippets are varying in size and content. They can be either rough (e.g., rocks), smooth (e.g., sky), or structured (e.g., buildings). The size of the images in this dataset is large, varying from 420×300 to 3888×2592. Around 10% of the pixels in the image belong to forged regions. Both geometric operations such as rotation and scaling and post-processing operations such as additive noise and JPEG compression have been applied to forged regions. Ground truth is available for this dataset. The details of this dataset are given in Table 1.

4.2. Evaluation metrics

CMFD is treated as a classification problem, where image pixels or entire images are classified either as forged or authentic. To

Table 1
Subsets in image manipulation dataset.

Subset	Contents	Definitions	Total #Images
Original	48 high resolution images	Images without any modifications	48
Plain	Copy-move forgery	No geometric or post processing operations utilized	48
Additive noise	Copy-move with added Gaussian noise	Five levels of noise applied	240
JPEG compression	Copy-move with added JPEG artifacts.	Nine quality factors of JPEG applied (20% to 100%)	432
Rotation	Copy-move with slight rotation	2° to 10° with step length of 2°	240
Scaling	Copy-move with slight scaling	0.91 to 1.09 with step length of 0.02	480
Multi paste	Copied regions that pasted multiple times	Block of size 64x64 pixels was randomly pasted	48

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University –
Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

evaluate the performance of the proposed method, the evaluation approach in (Christlein et al., 2012) is adopted. At the image level, the important measures are as following:

- TP (True Positive): Correctly detected forged images.
- FP (False Positive): authentic images that detected incorrectly as forged images.
- FN (False Negative): forged images that incorrectly omitted as forged images.
- TN (True Negative): Correctly detected authentic images.

From these measures, various metrics' evaluation such as Precision, Recall and False Positive Rate (FPR) can be computed. Precision is the probability that a detected forgery is a forgery. The Recall is the fraction of tampered images that detected correctly, while FPR is the fraction of authentic images that are detected incorrectly. In our work, the image is considered as forged if at least a match is found between two image regions. The above-mentioned evaluation metrics are defined as:

$$\text{precision} = \frac{TP}{TP + FP} \tag{5}$$

$$\text{recall} = \frac{TP}{TP + FN} \tag{6}$$

$$\text{FPR} = \frac{FP}{FP + TN} \tag{7}$$

In addition, the F1 score is used as an evaluation metric, which merges precision and recall into a single value because there is no desired balance between recall and precision:

$$F_1 = 2.\frac{precision.recall}{precision + recall} \tag{8}$$

Based on these evaluation metrics the performance of proposed method on both MICC-F220 dataset and Image Manipulation dataset is evaluated, which will be illustrated in the next sections.

4.3. Results on MICC-F220 dataset

Firstly, the detection performance of our approach in terms of outlier removal is tested based on two cases: when applying RANSAC algorithm only and when applying GORE-RANSAC. The results proved that using of GORE algorithm provides a low FPR while preserving a high rate of correct tampering detection. The comparison results between both cases are given in Table 2.

Furthermore, the effect of the following algorithms CLAHE, SIFT and DBSCAN in the overall performance of the proposed method has been tested. First, the detection performance of the proposed method has been tested without applying CLAHE in the preprocessing stage. Second, SIFT algorithm has been replaced with SURF in the feature extraction and description stage. Finally, AHC is applied instead of DBSCAN for clustering. The detection performance results for these different algorithms applied to different stages are shown in Table 3 in terms of TPR and FPR. The results show that applying CLAHE, SIFT, and DBSCAN obtain the highest TPR value and the lowest FPR value. ·Note that each test was done separately (i.e., totally three tests were done and on each time one algorithm was removed or replaced in one stage while maintaining the rest of stages as they are).

Table 2
TPR and FPR values on MICC-F220 with respect to filtering methods.

Method	TPR (%)	FPR (%)
RANSAC	100	9.09
GORE-RANSAC	100	3.63

Table 3
Detection performance of testing the effect of different algorithms in the different stages.

Algorithm	Stage	TPR (%)	FPR (%)
Without CLAHE	Preprocessing	99.09	10.91
SURF	Feature extraction and description	82.73	10.71
AHC	Clustering	90.00	8.18

Table 4
Comparison evaluation on MICC-F220.

Methods	TPR (%)	FPR (%)
(Amerini et al., 2011)	100	8
(Kaur et al., 2015)	97.27	7.27
(Dadkhah et al., 2017)	97.8	5.6
(Abdel-Basset et al., 2018)	97.87	7.63
Proposed	100	3.63

For this dataset, the performance of the proposed method is compared with the following state-of-the-art methods: (Amerini et al., 2011), (Kaur et al., 2015), (Dadkhah et al., 2017), (Abdel-Basset et al., 2018). The detection performance results are shown in Table 4 in terms of TPR and FPR. Experiment results show that the proposed method and the method presented in (Amerini et al., 2011) achieve higher TPR values while the proposed method obtains the lowest FPR value. Some of the detection results including various attacks on this dataset are shown in Fig. 5 (a) and (b). Coordinates values of the detected keypoints after sift feature extraction stage are shown in Fig. 5(c).

4.4. Results on image manipulation dataset

In the proposed method, three scenarios have been considered when examining the detection performance of the proposed method on this dataset: (i) ideal condition (plain copy-move), (ii) under different attacks (iii) under multiple copy-move forgeries. In the first case, the performance of the proposed method is evaluated by comparing the results with other CMFD methods including: (Cozzolino et al., 2015), (Wang et al., 2016), (Yu et al., 2016), (Bi and Pun, 2017), (Jin and Wan, 2017), (Bi et al., 2018) and (Pun and Chung, 2018). The experimental results show that the proposed method has surpassed former CMFD methods in terms of precision, recall and, F-score (see Table 5). Section 4.4.1, illustrates the robustness of the proposed method under various attacks either intermediate or post-processing attacks. In addition, the ability of the proposed method to handle multiple copy-move forgeries are studied in subsection 4.4.2. Some of the detection results including various attacks on this dataset are shown in Fig. 6. Table 6 reports the running time of the proposed copy-move forgery detection method and compares it with other relevant methods.

4.4.1. Forgery detection results under different attacks

Besides the plain copy-move forgery, the proposed method has also tested when the copied regions are attacked by different attacks including geometric operations and post-processing operations. The copied regions are distorted by these attacks as follows:

- Gaussian noise:

The Gaussian noise is applied to the copied regions, by adding zero-mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10, separately. In this case, totally $48 \times 5 = 240$

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

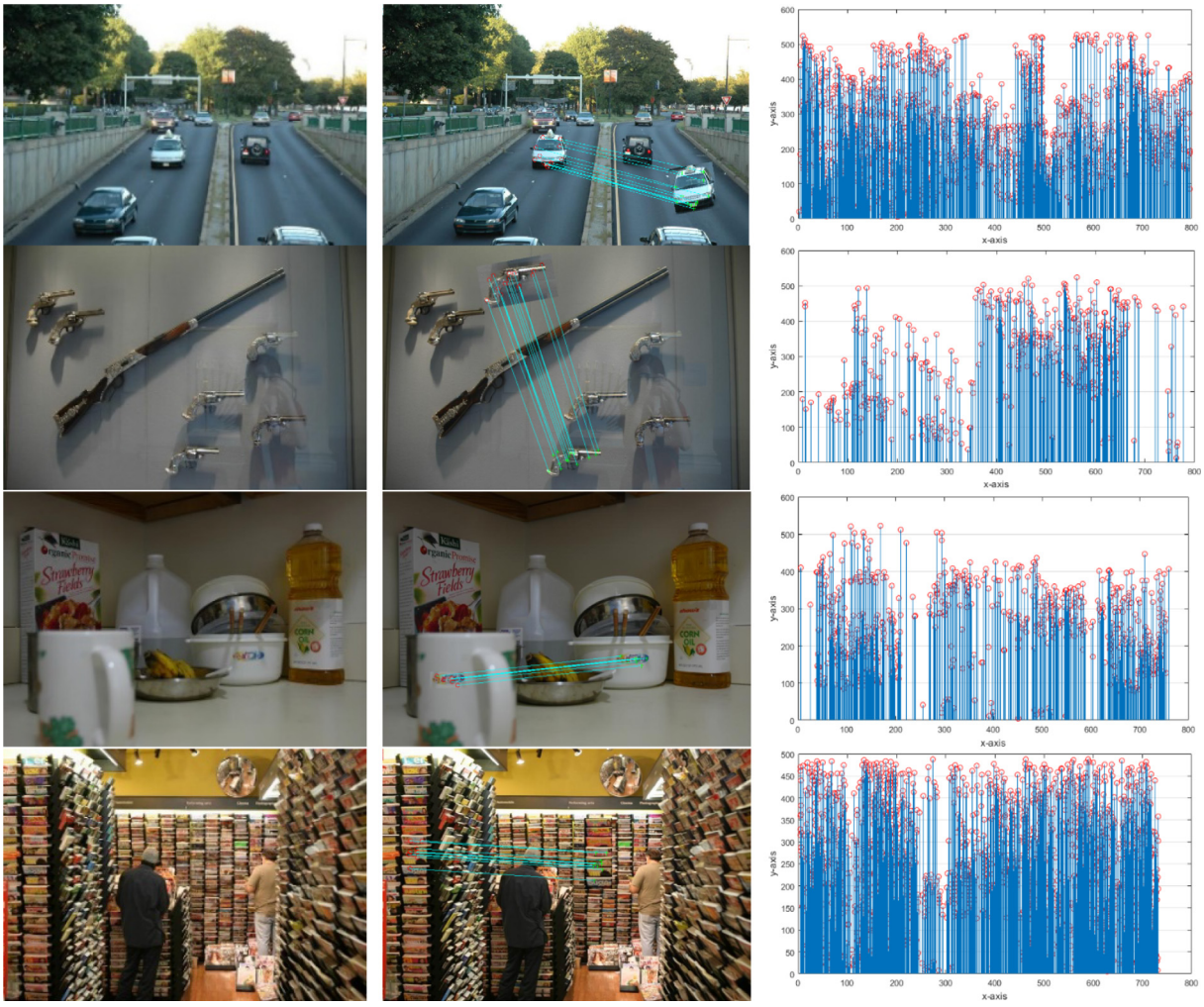

Fig. 5. Detection results on MICC-F220 under various attacks and the x-y coordinates of the detected keypoints.

Table 5
Detection results of the plain copy-move forgery.

Methods	F_1(%)
(Amerini et al., 2011)	79.2
(Cozzolino et al., 2015)	94.67
(Wang et al., 2016)	96.80
(Yu et al., 2016)	95.9
(Jin and Wan, 2017)	91.9
(Bi and Pun, 2017)	96.63
(Bi et al., 2018)	95.05
(Pun and Chung, 2018)	94.7
Proposed	97.56

images have tested. As the standard deviations increase, the number of false negatives also increases. Since high values lead to clearly visible artifacts, the SIFT algorithm cannot extract enough keypoints for matching. Hence, it affects the whole subsequent processing. The experimental results exhibit that the proposed method maintains high recall value as shown in Table 7.

- JPEG compression:

The copied regions are attacked by JPEG compression using quality factors 100 and 20 in step length of 10. In this case, there are totally 432 images tested. When the quality factor goes low, the real image quality is reduced. Images under JPEG compression of low-quality factors result in more false positives. The experimental results exhibit that the proposed method recall remains stable (see Table 7).

- Rotation-invariance:

The copied regions were attacked using rotation transforms with rotation degrees 2° to 10° with a step length of 2°. In this case, there are totally 240 images tested.

- Scaling-invariance:

Scaling factors between 91% and 109% with a step length of 2% are applied to the copied regions. In this case, totally 480 images have tested.

Since the SIFT algorithm generally is known for its strong invariance to rotation and scaling, even for large amounts, the proposed method maintains high recall under both attacks (see Table 7). Moreover, the proposed method is compared with other existing state-of-the-art methods.

From the above experimental results, the proposed method achieves better detection results for copy-move forgery images

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

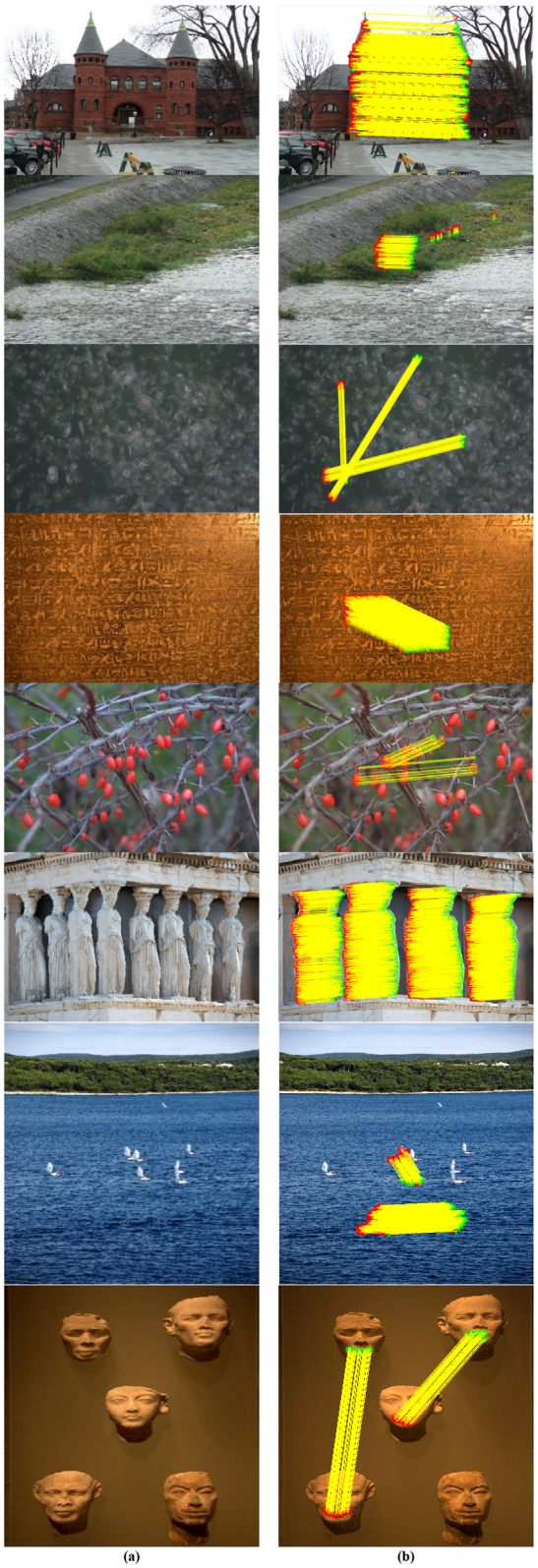

Fig. 6. Image Manipulation Dataset forged images are show in first column (a), corresponding forgery detection results are shown in (b).

under various attacks, such as geometric operations, and post-processing operations, compared with the existing state-of-the-art copy-move forgery detection methods as illustrated in Table 7. The proposed method exhibits better results due to several reasons: 1) by utilizing CLAHE in the preprocessing stage, more keypoints have been extracted from smooth regions. 2) SIFT features are invariant to scaling and rotation and provides a robust matching across the essential range of affine distortion, JPEG compression, noise addition, illumination change. 3) applying FANN and DBSCAN algorithms improved copy-move forgery detection in high dimensional data points. 4) two-stage outlier removal based on GORE and RANSAC is utilized to reduce falsely detected matched pairs and thus improve forgery detection.

Table 6
Processing Time of the proposed method and the state-of-the-art methods.

Methods	Processing Time (s)
(Amerini et al., 2011)	10112.16
(Wang et al., 2016)	9626.52
(Yu et al., 2016)	21576.08
(Pun and Chung, 2018)	8799.50
Proposed	7193.90

Table 7
Comparison results under various attacks on Image Manipulation Dataset.

Method	Recall (%)			
	Gaussian noise	JPEG compression	Rotation	Scaling
(Amerini et al., 2011)	40.4	41.7	46.7	59.6
(Yu et al., 2016)	79.4	80.7	98.6	86.4
(Bi et al., 2018)	69.2	67.2	91.2	91.6
Proposed	97.9	99.1	100	100

4.4.2. Detection results under multiple copies

Copy-move forgery is usually done by copying and pasting regions multiple times in the same image. When forged images have multiple copies, it becomes more challenging for CMFD methods to handle. For this reason, the proposed method is also evaluated when the forged images have multiple copies. In multi paste subset of image manipulation dataset, a block size of 64×64 pixels has been selected and randomly copied five times for the 48 images. Typically, as the arbitrary choice of small blocks often yields regions with very few matched keypoints, the performance of SIFT will decrease. This, in turn, affects the whole subsequent processing. The proposed method achieves a good result with a 95.83% recall.

4.5. Conclusion

In this paper, an improved SIFT features based method has been presented for copy-move forgery detection. The main contributions of this work are introducing a density-based clustering algorithm and Guaranteed Outlier Removal algorithm that can effectively reduce false matches. Various datasets have been tested containing different typologies and resolutions of fake and original images. Experimental results exhibit that the proposed technique performs well in the existence of various attacks such as scaling, rotation, a composition of these attacks, JPEG compression and Gaussian noise compared to other similar state-of-the-art techniques. Moreover, it can handle multiple copy-move forgeries with the least false matches.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University –
Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007

References

Abdel-Basset, Mohamed, Manogaran, Gunasekaran, Fakhry, Ahmed E., El-Henawy, Ibrahim, 2018. 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimedia Tools Appl. 1–19. https://doi.org/10.1007/s11042-018-6266-0.

Al-Qershi, Osamah M., Khoo, Bee Ee, 2013. Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Sci. Int. 231 (1–3), 284–295. https://doi.org/10.1016/j.forsciint.2013.05.027.

Alkawaz, Mohammed Hazim, Sulong, Ghazali, Saba, Tanzila, Rehman, Amjad, 2018. Detection of copy-move image forgery based on discrete cosine transform. Neural Comput. Appl. 30 (1), 183–192. https://doi.org/10.1007/s00521-016-2663-3.

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G., 2011. A SIFT-based forensic method for copy–move attack detection and transformation recovery. IEEE Trans. Inform. Forensic Secur. 6 (3), 1099–1110. https://doi.org/10.1109/TIFS.2011.2129512.

Amerini, Irene, Ballan, Lamberto, Caldelli, Roberto, Del Bimbo, Alberto, Del Tongo, Luca, Serra, Giuseppe, 2013. Copy-move forgery detection and localization by means of robust clustering with J-linkage. Signal Process. Image Commun. 28 (6), 659–669. https://doi.org/10.1016/j.image.2013.03.006.

Asghar, Khurshid, Habib, Zulfiqar, Hussain, Muhammad, 2017. Copy-move and splicing image forgery detection and localization techniques: a review. Aust. J. Forensic Sci. 49 (3), 281–307. https://doi.org/10.1080/00450618.2016.1153711.

Bakiah, Nor, Warif, Abd, Wahid, Ainuddin, Wahab, Abdul, Yamani, Mohd, Idris, Idna, Ramli, Roziana, Salleh, Rosli, Shamshirband, Shahaboddin, 2016. Copy-move forgery detection : survey, challenges and future directions. J. Netwk. Computer Appl. 75, 259–278. https://doi.org/10.1016/j.jnca.2016.09.008.

Bi, Xiu Li, Pun, Chi Man, Yuan, Xiao Chen, 2018. Multi-scale feature extraction and adaptive matching for copy-move forgery detection. Multimedia Tools Appl. 77 (1), 363–385. https://doi.org/10.1007/s11042-016-4276-3.

Bi, Xiuli, Pun, Chi Man, 2017. Fast reflective offset-guided searching method for copy-move forgery detection. Inf. Sci. 418–419, 531–545. https://doi.org/10.1016/j.ins.2017.08.044.

Bi, Xiuli, Pun, Chi Man, Yuan, Xiao Chen, 2016. Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. Inf. Sci. 345, 226–242. https://doi.org/10.1016/j.ins.2016.01.061.

Bustos, Alvaro Parra, Chin, Tat Jun, 2015. Guaranteed outlier removal for rotation search. IEEE Int. Conf. Comput. Vision 2165–73. https://doi.org/10.1109/ICCV.2015.250.

Christlein, Vincent, Riess, Christian, Angelopoulou, Elli, 2010. A study on features for the detection of copy-move forgeries. Sicherheit 105–16. https://doi.org/10.7566/JPSJ.82.124714.

Christlein, Vincent, Riess, Christian, Jordan, Johannes, Riess, Corinna, Angelopoulou, Elli, 2012. An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. 7 (6), 1841–1854. https://doi.org/10.1109/TIFS.2012.2218597.

Cozzolino, Davide, Poggi, Giovanni, Verdoliva, Luisa, 2015. Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. 10 (11), 2284–2297. https://doi.org/10.1109/TIFS.2015.2455334.

Dadkhah, Sajjad, Koppen, Mario, Sadeghi, Somayeh, Kaori Yoshida, H.A., Jalab, and Azizah Abdul Manaf, 2017. An efficient ward-based copy-move forgery detection method for digital image forensic. Int. Conf. Image Vision Comput. New Zealand 1–6. https://doi.org/10.1109/IVCNZ.2017.8402472.

Ester, Martin, Kriegel, Hans-Peter, Sander, Jörg, Xiaowei, Xu., 1996. A density-based for descovering clusters in large spatial databases with noise. In: 2nd International Conference on Knowledge Discovery and Data Mining, pp. 226–231. https://doi.org/10.1016/B978-044452701-1.00067-3.

Fischler, Martin, Bolles, Robert C., 1981. Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography. Commun. ACM 24 (6), 381–395. https://doi.org/10.1145/358669.358692.

Fridrich, Jessica, Soukal, David, Lukáš, Jan, 2003. Detection of copy-move forgery in digital images. Digital Forensic Res. Workshop 3 (2), 652–663. https://doi.org/10.1109/PACIIA.2008.240.

Hayat, Khizar, Qazi, Tanzeela, 2017. Forgery detection in digital images via discrete wavelet and discrete cosine transforms. Comput. Electr. Eng. 62, 448–458. https://doi.org/10.1016/j.compeleceng.2017.03.013.

Jin, Guonian, Wan, Xiaoxia, 2017. An improved method for SIFT-based copy-move forgery detection using non-maximum value suppression and optimized J-linkage. Signal Process. Image Commun. 57, 113–125. https://doi.org/10.1016/j.image.2017.05.010.

Kaur, Harpreet, Saxena, Jyoti, Singh, Sukhjinder, 2015. Simulative comparison of copy-move forgery detection methods for digital images. Int. J. Electron. 4, 62–66. http://academicscience.co.in/admin/resources/project/paper/f201509201442750218.pdf.

Khan, Shaharyar, Saleem, Zahra, 2018. A comparative analysis of SIFT SURF KAZE AKAZE ORB and BRISK. Int. Conf. Comput. Math. Eng. Technol. 1–10. https://doi.org/10.1109/ICOMET.2018.8346440.

Kumar, R., Sharma, H., 2008. Comparative study of CLAHE, DSIHE & DHE Schemes. Int. J. Res. Manage. Sci. Technol. 1 (1), 1–4, papers://b6c7d293-c492-48a4-91d5-8fae456be1fa/Paper/p12626.

Li, Jian, Li, Xiaolong, Yang, Bin, Sun, Xingming, 2015. Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. 10 (3), 507–518. https://doi.org/10.1109/TIFS.2014.2381872.

Lin, Xiang, Li, Jian Hua, Wang, Shi Lin, Liew, Alan Wee Chung, Cheng, Feng, Huang, Xiao Sa, 2018. Recent advances in passive digital image security forensics: a brief review. Engineering 4 (1), 29–39. https://doi.org/10.1016/j.eng.2018.02.008.

Lowe, David G., 2004. Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vision 60 (2), 91–110. https://doi.org/10.1023/B:VISI.0000029664.99615.94.

Ma, Jinxiang, Fan, Xinnan, Yang, Simon X, Zhang, Xuewu, Zhu, Xifang, 2017. Contrast limited adaptive histogram equalization based fusion for underwater image enhancement. Preprints 127. https://doi.org/10.20944/preprints201703.0086.v1.

Muja, Marius, Lowe, David G., 2009. Fast approximate nearest neighbors with automatic algorithm configuration. In: VISAPP International Conference on Computer Vision Theory and Applications, pp. 331–340. https://doi.org/https://10.5220/0001787803310340.

Pun, Chi Man, Chung, Jim Lee, 2018. A two-stage localization for copy-move forgery detection. Inf. Sci. 463–464, 33–55. https://doi.org/10.1016/j.ins.2018.06.040.

Qureshi, Muhammad Ali, Deriche, Mohamed, 2015. A bibliography of pixel-based blind image forgery detection techniques. Signal Process. Image Commun. 39 (Part A), 46–74. https://doi.org/10.1016/j.image.2015.08.008.

Sia, Nicholas, Kong, Pik, Ibrahim, Haidi, Hoo, Seng Chun, 2013. A Literature review on histogram equalization and its variations for digital image enhancement. Int. J. Innov. Manage. Technol. 4 (4), 386–389. https://doi.org/10.7763/IJIMT.2013.V4.426.

Ng, Tian-Tsong, Chang, Shih-Fu, Hsu, Jessie, Pepeljugoski, Martin, 2005. Columbia photographic images and photorealistic computer graphics dataset. ADVENT Techn. Rep., 205–2004

Wang, Xiang-yang, Li, Shuo, Liu, Yu-nan, Niu, Ying, Yang, Hong-Ying, Zhou, Zhi-li, 2016. A new keypoint-based copy-move forgery detection for small smooth regions. Multimedia Tools Appl. 76 (22), 23353–23382. https://doi.org/10.1007/s11042-016-4140-5.

Yang, Bin, Sun, Xingming, Guo, Honglei, Xia, Zhihua, Chen, Xianyi, 2018. A copy-move forgery detection method based on CMFD-SIFT. Multimedia Tools Appl. 77 (1), 837–855. https://doi.org/10.1007/s11042-016-4289-y.

Yang, Fan, Li, Jingwei, Wei, Lu., Weng, Jian, 2017. Copy-Move Forgery Detection Based on Hybrid Features. Eng. Appl. Artif. Intell. 59, 73–83. https://doi.org/10.1016/j.engappai.2016.12.022.

Yu, Liyang, Han, Qi, Niu, Xiamu, 2016. Feature point-based copy-move forgery detection: covering the non-textured areas. Multimedia Tools Appl. 75 (2), 1159–1176. https://doi.org/10.1007/s11042-014-2362-y.

Please cite this article as: A. Hegazi, A. Taha and M. M. Selim, An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal, Journal of King Saud University –
Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007