International Journal of Sociotechnology and Knowledge Development
Volume 12 • Issue 1 • January-March 2020

Copy-Move Forgery Detection Based on Automatic Threshold Estimation

Aya Hegazi, Faculty of Computers and Informatics, Benha University, Benha, Egypt
Ahmed Taha, Faculty of Computers and Informatics, Benha University, Benha, Egypt
Mazen Mohamed Selim, Faculty of Computers and Informatics, Benha University, Benha, Egypt

ABSTRACT

Recently, users and news followers across websites face many fabricated images. Moreover, it goes far beyond that to the point of defaming or imprisoning a person. Hence, image authentication has become a significant issue. One of the most common tampering techniques is copy-move. Keypoint-based methods are considered as an effective method for detecting copy-move forgeries. In such methods, the feature extraction process is followed by applying a clustering technique to group spatially close keypoints. Most clustering techniques highly depend on the existence of a specific threshold to terminate the clustering. Determination of the most suitable threshold requires a huge amount of experiments. In this article, a copy-move forgery detection method is proposed. The proposed method is based on automatic estimation of the clustering threshold. The cutoff threshold of hierarchical clustering is estimated automatically based on clustering evaluation measures. Experimental results tested on various datasets show that the proposed method outperforms other relevant state-of-the-art methods.

KEYWORDS

Clustering Evaluation Measures, Copy-Move Detection, Image Forensics, Keypoint-Based Methods, Multiple-Copied Matching

1. INTRODUCTION

Digital images are everywhere, and they have the power to do infinitely more than a document. In the latter half of the last two decades, the internet, mobile technology, and obsession of social media have highly affected and changed people's lives (Katta & Patro, 2017; Mahajan et al., 2018; Muliawat et al., 2019). Recently, there is a rapid increase in images showing in the media as in social media and television that don't seem to be all as they appear. Authenticity of digital images is a critical issue. Day by day, it becomes easy for anyone to manipulate images even without leaving any visible clues. Wide availability of powerful image processing software like Photoshop and Gimp makes it more challenging for digital image authentication.

Digital image forensics is the science of detecting tampered regions in images. Identifying the authenticity of digital images is very important in digital forensics. The purpose of digital image manipulation is to conceal or hide information for several intentions therefore change their meaning. Many areas have been affected by digital forensics. The impact of image manipulation in media, journalism, digital cinema, news and in politics to mislead the public opinion. It could also be used in law for miscarrying justice. Manipulated images also have been found in academic papers. In a survey by Tijdink (Tijdink et al., 2014), in the past three years, 15% of offenders are involved in scientific

DOI: 10.4018/IJSKD.2020010101

misconduct such as fabricating, refutation or manipulating data. A study by (Farid, 2006) reported that in the Journal of Cell Biology about 20% of admitted manuscripts have at least one figure that must be restored due to unsuitable image manipulation, and about 1% are deceitful figures. These consequences make image authenticities less trustful.

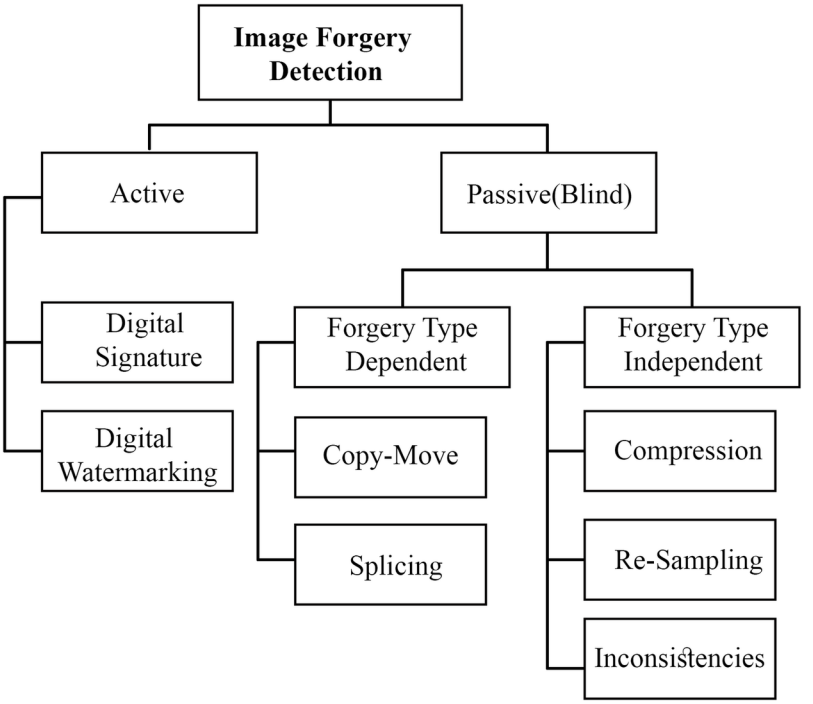
Rapid growth of forged images and their influence in many areas have led to the development of tampering detection techniques. Tampering detection techniques fall under two categories: active authentication and passive authentication methods (Al-Qershi & Khoo, 2013) as shown in Figure 1. Active authentication methods require some preprocessing on digital images like watermarking, or signatures. Digital watermarking conceals a watermark into the image at the capturing end and extracts it at the authentication end to examine whether the image has been tampered with (Al-Qershi & Khoo, 2013). Inserting the watermark either at the capturing time of the image using a specially equipped camera or later by an authorized person is the main drawback of watermarking (Qureshi & Deriche, 2015). Moreover, most of the cameras today are not equipped with a watermark embedding technique. In addition, the subsequent processing of the original image could degrade the image visual quality. Moreover, digital signature is similar to digital watermarking. At the image-capturing end, unique features are extracted from the image as a signature. At the authentication and detection end, the signature is regenerated using the same method and the authenticity of the image can be identified and verified through comparison. Digital signatures have the same drawbacks of digital watermarking.

On the other hand, Passive (blind) authentication methods authenticate images while not requiring any previous information of it. It relies on the traces left on the image during manipulation by various processing operations. Therefore, passive authentication methods are considered as the most common (Lin et al., 2018). Passive detection techniques can be classified to forgery-type dependent or forgery-type independent. Forgery-type independent techniques detect forgeries regardless of the type of the forgery. To detect general tampering, the independent techniques exploit three diverse types of artifacts: traces of re-sampling, compression and inconsistencies (Redi et al., 2011). The forgery-type dependent techniques are used for certain types of forgeries. Copy-move and splicing are examples of forgery-type dependent (see Figure 1). Such techniques depend on copying and pasting image regions either from the same image (copy-move), or from different images (splicing). Image splicing is created from at least two different images (Sharma & Ghanekar, 2019; Walia & Kumar, 2018). An Example of image splicing is shown in Figure 2(d).

Copy-move or cloning is a technique of copying a region and pasting it in the same image. It contains at least two regions alike (see Figure 2(b)). Since the duplicated regions are from the same image, they inherit the same basic image properties such as color palette, illumination conditions and noise. Copy-move forgery is the most common type used for image manipulation due to its simplicity and effectiveness (Al-Qershi & Khoo, 2013; Bakiah et al., 2016). Although this technique is easy to implement, it is hard to detect. Often in practice, forgery is not just limited to copying and pasting the regions, some processing operations are applied to these regions. These operations can be classified to intermediate operations (geometric transformations) and post-processing operations. Intermediate operations are used to provide a spatial synchronization and homogeneity between the copied region and its neighbors (Al-Qershi & Khoo, 2013; Bakiah et al., 2016). Examples of intermediate operations are rotation and scaling. Post-processing operations are used to remove traces left from forgery and to make it unnoticeable. Additive noise, JPEG compression and blurring are examples of post-processing operation (Liu et al., 2010). Since all those operations make detecting copy-move forgery more challenging, numerous methods have been proposed for Copy-Move Forgery Detection (CMFD). Most of them can be classified either into block-based methods or keypoint-based methods (Bakiah et al., 2016). In block-based methods, the image is divided into overlapping or non-overlapping blocks of fixed size. On the other hand, keypoint-based methods calculate local interest points (keypoints) from the whole image without any subdivisions.

Generally, CMFD techniques follow a common pipeline as shown in Figure 3 (Christlein et al., 2012). Both block-based and keypoint-based methods follow the same pipeline steps except for

Figure 1. Existing image forgery detection techniques



feature extraction. The first stage of CMFD pipeline is preprocessing. It is an optional stage and it depends on the technique used. It aims to improve the image data either by enhancing the image features or by removing some unwanted distortion. Converting RGB image to grayscale is one of the most used methods for pre-processing (Bakiah et al., 2016). After this conversion, features are extracted either from the divided blocks in block-based methods or for the keypoints then they are stored in a feature vector. In the matching stage, each feature vector is compared with each other to find similarities within the same image. In this stage once the matched blocks are detected, copy-move forgery manipulations are determined. The matching technique used depends on the extracted features of block-based or keypoint-based methods. In the filtering process, outliers and false matches are removed. Finally, the copy-move forgery detection result can be visualized to localize the tampered regions in the forged image. Visualization can be further refined by morphological operation such as filling the holes. There is always a motivation for presenting a copy-move detection technique with efficient complexity and robustness against image processing operations.

The rest of the paper is structured as follows. Section 2 introduces related work. Section 3 explains our proposed method. The experimental results are given in section 4. Finally, section 5 concludes the paper.

2. RELATED WORK

In the literature, several techniques in both block-based and keypoint-based have been introduced for copy-move forgery detection. Among the block-based methods, Discrete Cosine Transform (DCT) is considered as the most widely used. (Fridrich et al., 2003) suggest the first method for detecting copy-move forgery; they used 256 coefficients of DCT as features. Further improvements based on DCT have been introduced in (Cao et al., 2011b, 2011a; Hu et al., 2011; Junhong, 2010). Although

Figure 2. Examples of blind forgery: (a) and (c) Original images; (b) Copy-move forged image; (d) Spliced forged image

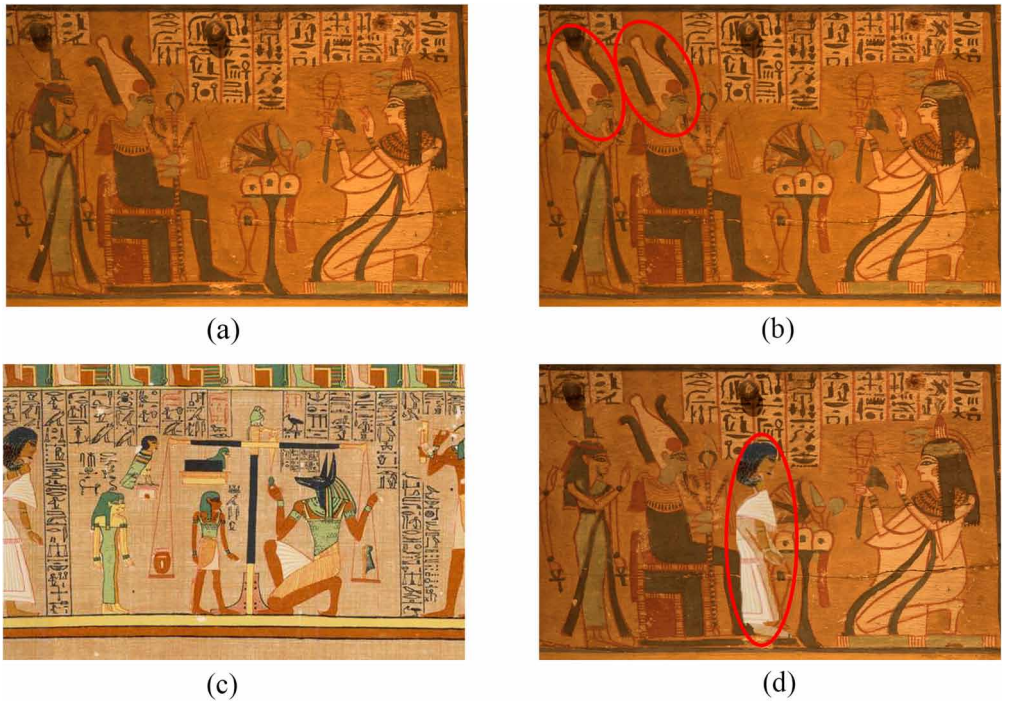
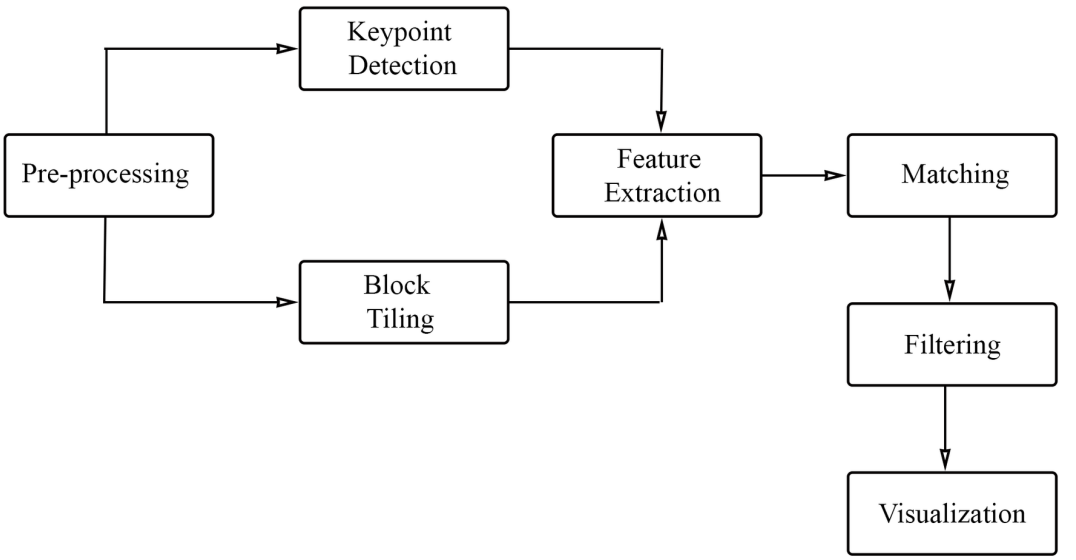


Figure 3. Common processing pipeline for copy-move forgery detection



block-based methods are robust to noise and JPEG compression, they are sensitive to geometric transformations like rotation and scaling and often result in significant false positives. Moreover, they have large feature vector size. It results in a high computational complexity (Christlein et al., 2012). In contrast, keypoint-based methods outperform block-based methods. They match features of the

image instead of blocks. Hence, it results in less computational complexity and minimum memory consumption (Dada et al., 2016).

On the other hand, keypoint-based methods exhibit the most accurate and stable results in the presence of geometrical transformations (e.g. scaling, rotation, and affine transformation). Scale-Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF) are most widely used keypoint-based methods. (Amerini et al., 2011) introduce a SIFT-based method in which feature vectors are extracted by SIFT. Then, they are matched using generalized 2-nearest neighbor (g2NN) algorithm followed by agglomerative hierarchical clustering. Although this method can deal with multiple copy-move forgery, it fails to localize copy move regions accurately. In addition, it is unable to separate duplicated regions that are near one another. Moreover, sometimes clustering could be unacceptable because it needs to set an empirical threshold to stop the process.

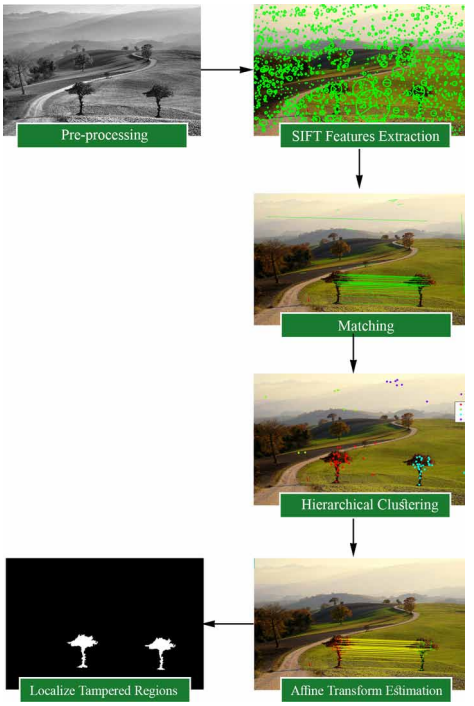
Shivakumar and Baboo (B.L.Shivakumar & Baboo, 2011) used Harris detector as keypoints detector while SIFT is used as a descriptor. The k-dimensional tree (kd-tree) algorithm is utilized for matching keypoints and for detecting duplicated regions. Pan and Lyu (Pan & Lyu, 2010) present another SIFT-based detection algorithm. The detected SIFT keypoints are matched using the best-bin-first algorithm followed by Random Sample Consensus (RANSAC) algorithm for geometric tampering estimation. However, quantitative results on a realistic dataset are not offered and cannot accurately detect tampered regions because of the lack of correct matched points. This method has a deficient performance when detecting small duplicate regions. In (Li et al., 2015), they present a method based on SIFT and segmentation. They suggest the use of EM algorithm for transform estimation refinement to reduce false matches. However, their method suffers from high computational complexity. Their work is tested using two datasets and cannot detect plain copy-move forgery accurately. Moreover, they identified some unforged images as forged. Yang et al. (Yang et al., 2017) present a method based on hybrid features. They used interest point detector called KAZE combined with SIFT for feature extraction. KAZE is a Japanese word that means wind.

Although keypoint-based methods record a good performance, they still suffer from several issues that critically affect the tampering detection. Most prior methods empirically select thresholds and do not consider its relationship with the image and forged region size. Furthermore, they cannot detect enough keypoints in flat areas, which result in many false negatives and inaccurate localization. Generally, an effective and efficient copy-move forgery detection technique should be robust to image processing operation (i.e. intermediate and post-processing operations). Moreover, it should accurately localize tampered regions and attain less computational complexity.

3. PROPOSED METHOD

The proposed method detects copy-move forgery based on SIFT features and agglomerative hierarchical clustering. The estimation of threshold that can effectively and efficiently handle the most common issues related to keypoint-based methods is done automatically. In our experiment, CLAHE based on Rayleigh distribution function is applied. Clip limit and tile size are set to 0.01 and 4×4 respectively. As shown in Figure 4, the whole detection process of the proposed method. In our detection scheme, the image is first preprocessed. Then, features are extracted using SIFT. Distinctive SIFT keypoints are then matched between each other using fast approximate nearest neighbor method. After that, hierarchical clustering is applied on the matched points. Finally, the image is filtered, and tampered regions are localized. Each step of the detection method will be described in detail in the following subsections: section 3.1 describes the image preprocessing, section 3.2 introduces SIFT features extraction, section 3.2 illustrates keypoint matching, section 3.3 presents the clustering and forgery detection, section 3.4 shows the process of estimating affine transformation and finally section 3.5 illustrates how tampered regions are localized.

Figure 4. Framework of the proposed copy-move forgery detection method



3.1. Image Preprocessing by CLAHE

As mentioned earlier, SIFT feature extraction algorithm cannot detect enough keypoints in flat areas. To limit this issue, in our work, Contrast-Limited Adaptive Histogram Equalization (CLAHE) (Ma et al., 2017) is used to enhance the contrast of the image. CLAHE is locally adaptive contrast enhancement method. In contrast to global HE, CLAHE works locally in small areas called tiles as opposed to the entire image. Each tile's contrast is improved, so that the processed histogram region approximately matches the histogram specified by a distribution function (e.g. uniform, Gaussian, or Rayleigh). Before computing the Cumulative Distribution Function (CDF) in CLAHE, the histogram is clipped at a specific value which limits the noise amplification. CLAHE depends on two main parameters: Block (tile) Size and Clip Limit. The quality of the improved image is controlled mainly by these parameters. Rayleigh distribution is one of the commonly used histogram clips, which produce a bell-shaped histogram (Ma et al., 2017). Rayleigh distribution function is given by:

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

where y_{min} is the lower bound of the pixel value, α is a scaling parameter of Rayleigh, and $p\left(i\right)$ is cumulative probability which is provided to create transfer function. A higher value of α will result in more significant contrast enhancement in the image, increasing saturation value and amplification of noise levels.

Using CLAHE offers many advantages; easy to implement; simple calculation, and it provides good results in image's local areas. CLAHE can limit brightness saturation that usually results from HE and results in less noise (Kumar & Sharma, 2008).

It worth noticing that applying CLAHE generally on all images will not always result in satisfying results. Some image regions may become oversaturated or darker which will critically affect the tampering detection results. Thus, CLAHE will only be applied on low contrast images. In our experiment, CLAHE based on Rayleigh distribution function is applied. Clip limit and tile size are set to 0.01 and 4×4 respectively.

3.2. SIFT Features Extraction and Description

The proposed method is based on an effective keypoint detector and descriptor called Scale Invariant Feature Transform (SIFT) (Lowe, 2004). SIFT algorithm extracts distinctive features (or local features) in digital images that are invariant to image scaling and rotation and provide robustness to changes in illumination, distortion, noise addition, and 3D viewpoint (Lowe, 2004). It is applied to the input image to extract SIFT distinctive keypoints which are represented with 128-dimensional feature vector. As described in (Lowe, 2004), the following are the major stages of SIFT algorithm explained briefly:

- **Scale-space peak selection:** The goal of this stage is to identify locations and scales that can be frequently assigned under divergent views of the same object. That is done by detecting extrema using a difference of Gaussian function at different scales of the image;
- **Keypoint localization:** Some of keypoint candidates result from the previous stage are unstable (i.e. they lie along an edge, or they have a low contrast). For that a detailed model is fit to the nearby data for accurate location, scale, and contrast. So, unstable keypoints are rejected and hence increase the efficiency and the robustness of the algorithm. At the end of this stage obtained keypoints are stable and scale invariance. For more details, see (Lowe, 2004);
- **Orientation assignment:** Based on local image properties, one or more orientations are assigned to each keypoint. Around each keypoint gradient direction and magnitude are calculated. Then the most prominent gradient orientation(s) are identified and assigned to that region. Now, keypoints that are rotation invariance are obtained;
- **Keypoint descriptor:** After assigning location, scale and orientation for each keypoint, a descriptor is computed for the local image region based on a window around the detected keypoint. Therefore, the output of this step is a unique SIFT keypoints that are represented with 128-dimensional descriptor vectors. Keypoints descriptor is highly distinctive and it is invariant to scaling, rotation, illumination change and 3D viewpoint.

3.3. Keypoint Matching

In a copy-move forgery, keypoints extracted from the original and duplicated regions have the same descriptor vectors. Therefore, matching between them is applied to authenticate copy-move forgeries in the image. Usually matching between detected keypoints is done using g2NN as in (Amerini et al., 2013; Dada et al., 2016; Li et al., 2015; Mohamdian & Pouyan, 2013). Anyway, it is known to suffer from high complexity when identifying the similarity from many high dimensional vectors. In addition, it gives less accurate results especially in high dimensional space. Moreover, lexicographic sorting yields higher false negative rate (Christlein et al., 2010). To address these issues, Fast Approximate Nearest Neighbor (FANN) method introduced by Muja et al. (Muja & Lowe, 2009) is used. It is based on Best-Bin-First (BBF) search which is a variant of a KD-tree that is used for finding approximate nearest neighbors with highest probability and less time. In the work introduced in (Christlein et al., 2010), it has been shown that the use of KD-tree matching generally gives a better results compared to lexicographical sorting especially in very-high-dimensional space. The idea of BBF is to search in bins of kd-tree in order of distance from the query using a priority queue. The distance to a bin

(node) is the minimum distance between the query and any other point on the bin boundary. At each internal node visited store the position and the distance in the queue instead of backtracking, pop the closest distance from the queue and continue from it (Lowe, 2004).

Given a test image, a set of keypoints $F = \{f_1, \ldots, f_n\}$ and its corresponding descriptor $D = \{D_1, \ldots, D_n\}$ are extracted. Matching operation is performed between feature descriptors to identify the similarity between them. Features descriptor is used to build the KD-tree. After that BBF search is applied on the kd-tree to find the N nearest neighbors of each keypoint f_i from all other (n-1) keypoints of the image. Nearest neighbor is computed using Euclidean distance. Let sorted Euclidean distance which is known as similarity vector denoted by $d = \{d_1, d_2, \ldots, d_{n-1}\}$. As suggested by (Lowe, 2004), the ratio between the distance of closest neighbor to the distance of the second closest neighbor is calculated and then the result is compared to a predefined threshold *T* (usually range from 0.3 to 0.5) to reduce false matches. Therefore, the keypoint is matched only if the following constraint is satisfied:

$$d1 / d2 < T \quad where, T\epsilon (0,1) \tag{2}$$

Since copy-move forgeries may have same image area that is cloned multiple times, it is necessary to handle this case. FANN algorithm can manage multiple copy-move forgery. At the end of this stage, all the matched keypoints are kept and isolated, and ones are discarded.

3.4. Clustering and Forgery Detection

In order to identify possible forged regions and group spatially closed keypoints, Agglomerative Hierarchical Clustering (AHC) (Hastie et al., 2003) is applied on spatial locations of matched feature pairs. AHC is a bottom-up clustering method. Hierarchical clustering creates a hierarchy of clusters where clusters have sub-clusters, which in turn have sub-clusters, etc. It starts with each keypoint in its own singleton cluster. Pair-wise distances between clusters are then evaluated. It agglomerates (merges) the closest pair of clusters with shortest distance. This process is repeated until all clusters have been merged into a single cluster that contains all keypoints. AHC can be visualized using a tree-like diagram called a dendrogram. It shows the progressive grouping of the keypoints. It is then possible to determine what suitable number of clusters is. Generally, merging of the keypoints is determined by two criteria: the linkage method and the cutoff threshold used to stop clustering. Cutoff threshold plays a key role in forgery detection and it critically affects the results. Often, the problem of cutting off a dendrogram has been a difficult issue in hierarchical clustering researches (Abe et al., 2017). Usually, setting cutoff threshold requires many experiments and optimization as in (Amerini et al., 2011). Moreover, determining cutoff threshold is so tricky because of different size of images and different size of forged regions. To handle this issue, the proposed method uses dynamic cutoff, which automatically terminates the clustering process once optimal number of clusters are obtained. It estimates optimal number of clusters based on internal cluster validity measures. Generally, cluster validation is used to verify that any found cluster is really in data rather than being produced from algorithms artifacts (Everitt et al., 2011). Cluster validation can be divided into two main methods: Internal and external (Halkidi et al., 2002). Internal methods measure cluster quality based on inter-cluster separation and intra-cluster compactness (cohesion). In our work, two commonly used internal methods for AHC are introduced: gap statistics (Tibshirani, 2001) and silhouette width (Gan, 2007). The proposed method is compared using gap statistic and silhouette width (see sections 4.3 and 4.4 for a detailed description of such experiment). Mathematical details for both gap statistic and silhouette coefficient are given in section 3.4.1 and 3.4.2 respectively. For the linkage method, the "Ward" linkage is used in the proposed method as it gives the best results (Amerini et al., 2011).

Ward's method supposes that a cluster is represented by its centroid. The increase of Sum of Squares Error (SSE) that results from merging two clusters is used by Ward method to measure the proximity between two clusters. Sum of squares in AHC starts at zero (every point is in its own singleton cluster) and grows as merging the clusters. Ward's method attempts to minimize SSE distances of points from their cluster centroids to keep this growth as small as possible.

Given two clusters, A and B, the distance between them given by (Amerini et al., 2011):

$$\Delta_{dist}\left(A,B\right) = SSE\left(AB\right) - \left[SSE\left(A\right) + SSE\left(B\right)\right] \tag{3}$$

where:

$$SSE\left(A\right) = \sum_{i=1}^{n_A} \left| x_{Ai} - \overline{x}_A \right|^2 \tag{4}$$

where Δ is called the merging cost of combining the clusters A and B, n_A is number of points in cluster A, x_{Ai} indicates the ith point in cluster A, and $\overline{x}_A$ is the centroid.

3.4.1. Gap Statistic

The gap statistic (Tibshirani et al., 2001) is used to estimate the optimal number of clusters. The idea is that for different values of k clusters, the changes of the total within intra-cluster are compared with its expectation under a null hypothesis (i.e. a distribution with no clustering). Value of k that maximizes the gap statistic represents the estimation of the optimal number of clusters. This means that the structure of clustering is much far from the random uniform distribution of points. There are two choices of reference distribution either based on uniform distribution or based on principal component analysis (more details in (Tibshirani et al., 2001). For simplicity, in the proposed method, uniform reference distribution is used. The following are how gap statistics work briefly:

1. Cluster the data into k clusters with $C_r = \left\{C_1, C_2, \ldots, C_k\right\}$ denoting the indices of data in cluster r;

Compute the pairwise distance for all points in cluster r such that:

$$D_r = \sum_{i,i' \in C_r} d_{ii'} \tag{5}$$

Compute the total within intra-cluster such that:

$$w_k = \sum_{r=1}^{k} \frac{1}{2\ n_r}\ D_r \tag{6}$$

4. B reference data sets are generated based on a reference distribution method. Then every of those reference data sets is clustered into k clusters;
5. The corresponding total within intra-cluster variation $W_{kb}^*,\ b = 1,2,\ldots,B,\ k = 1,2,\ldots,K$ is computed;

The estimated gap statistic is computed:

$$Gap\left(k\right)=\frac{1}{B}\sum_{b=1}^{B}\log\left(\ W_{kb}^{*}\right)-\log\left(w_{k}\right) \tag{7}$$

Compute the standard deviation sd_k and define the standard error s_k:

$$sd_{k}=\left[\left(\frac{1}{B}\right)\sum_{b}\left\{\log\left(W_{kb}^{*}\right)-\overline{l}\right\}^{2}\right]^{\frac{1}{2}} \tag{8}$$

$$s_{k}\ =sd_{k}\sqrt{\left(1+\frac{1}{B}\right)} \tag{9}$$

where:

$$\overline{l}\ =\left(\frac{1}{B}\right)\sum_{b}\log\left(W_{kb}^{*}\right) \tag{10}$$

8. Finally, the smallest value of k is selected as the optimal the optimal number of clusters $\hat{k}$ in which the gap statistic is within one standard deviation of the gap at k+1:

$$\hat{k}=smallest\ \ k,such\ \ that\ \ Gap\left(k\right)\geq Gap\left(k+1\right)-s_{k+1}$$

3.4.2. Silhouette Width

The Silhouette width (Gan, 2007) can be used to represent the compactness and separation of clusters. It measures the closeness between every point in one cluster to the points within the neighboring clusters. For different values of k, the average Silhouette of observations is computed. Such that, the one that maximizes the average Silhouette over all potential k values represent the optimal number of clusters k. Suppose point x_i belongs to cluster k. First, let the average distance between this point and all others in the same cluster represented by a_i. Second, let the average distance between this point and those in cluster $l\neq k$ represented by d_{li}. Let the average distance between x_i and the nearest cluster of which it is not a member is denoted by, $b_i=min_l d_l$. Therefore, the Silhouette width is given by:

$$s\left(x_{i}\right)=\frac{b_{i}-ak_{i}}{\max\left[a_{i},b_{i}\right]} \tag{11}$$

Larger value of $s\left(x_i\right)$ means that x_i lies better in its cluster. Entire clustering structure is measured by the average Silhouette of all data points (also called Silhouette Width Criterion SWC). Best clustering structure corresponds to maximized SWC. It is given by:

$$SWC = \frac{1}{N}\sum_{i=1}^{N} s\left(x_i\right) \tag{12}$$

3.5. Affine Transform Estimation

Preliminarily, we know that image is tampered and where the source region and target (copy-moved) region. Since copy-move regions undergo geometric distortions (such as scaling, rotation), the relationship between tampered regions is estimated using affine transformation specified by a transformation matrix H. Given the coordinate of two corresponding matched points from a region and its duplicate as $X = \left(x, y\right)^T$ and $\tilde{X} = (\tilde{x}, \tilde{y})^T$, respectively. The geometric relationship between these two regions is expressed as:

$$\tilde{X} = HX \tag{13}$$

It can be expressed in matrix form as:

$$\begin{pmatrix} \tilde{x} \\ \tilde{y} \\ 1 \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \tag{14}$$

where the parameters a_{11}, a_{12}, a_{21}, a_{22}, are associated with scaling and rotation, while t_x, t_y are associated with translation. Since affine transformation has six degrees of freedom (six matrix parameters), there is a need for at least three matched pairs not to be collinear to obtain the affine transformation. Given a set of correspondences $\left(X_1, \ldots, X_n\right)$ and $\left(\tilde{X}_1, \ldots, \tilde{X}_n\right)$, the transformation matrix H can be computed by means of minimizing the following total error function:

$$\sum_{i=1}^{n} \left\| \tilde{X}_i - HX_i \right\|^2 \tag{15}$$

Mismatched points or outliers can solely affect the estimated homography H. In that case, a widely used method for robust estimation called Random Sample Consensus (RANSAC) (Fischler & Bolles, 1981) is employed to perform the previous estimation more accurately. This method is also adopted by some other CMFD techniques (Amerini et al., 2011; Dada et al., 2016). RANSAC randomly selects three pairs of points or more from the matched points and estimates the homography matrix H by minimizing the total error function given in equation (15). Then, according to H, all the remaining points are transformed. After that, all pairs of matched points are classified into inliers or outliers depending on the estimated matrix H. A pair of matched points considered as inlier if $\left\| \tilde{X} - HX \right\| \leq \beta$, otherwise, it is outlier. After N_i times of iteration, RANSAC returns the estimated transform

parameters that result in the biggest variety of inliers. In our experiment, β is set to 3 and N_i is set to 1000. Finally, a set of affine transformations $\left\{H_1,\ldots,H_n\right\}$ are acquired.

Estimation of affine transformation is an important stage of CMFD scheme. Falsely detected regions that do not have a set of points with uniform transform relationship, will be removed in this stage. Moreover, it enhances the detection of copy-move forgery by providing the more details about tampered image. In literature, most of recent CMFD methods choose to estimate geometric transformations (Amerini et al., 2011; Shivakumar & Baboo, 2011; Dada et al., 2016; Hashmi et al., 2014; Li et al., 2015).

3.6. Tampered Regions Localization

Once an image is considered as tampered, duplicated regions can be accurately localized. With the estimated affine transformation H, identical regions are found by comparing each pixel in the image with its transformational counterpart. In the proposed method, a localization method is used as in (Yang et al., 2017). Localizing tampered regions is illustrated in the following steps:

1. All points in the image are transformed forward with the matrix H and backward with the inverse matrix H^{-1} let original region R^o and its related tampered region R^F then the relation between these two regions in terms of transformation matrix is:

$$R^F = HR^o, \quad R^o = H^{-1}R^F$$

To localize the tampered regions, the similarity between the original image I and transformed (warped) image T is measured using Zero Mean Normalized Cross-Correlation (ZNCC). Let pixel intensities at location *x* denoted as $I\left(x\right)$ and $T\left(x\right)$, then:

$$ZNCC\left(x\right) = \frac{\sum_{v\in\Omega(x)}\left(I\left(v\right)-\bar{I}\right)\left(T\left(v\right)-\bar{T}\right)}{\sqrt{\sum_{v\in\Omega(x)}\left(I\left(v\right)-\bar{I}\right)^2\left(T\left(v\right)-\bar{T}\right)^2}}, ZNCC\in\left(0,1\right) \tag{16}$$

where $\Omega\left(x\right)$ a 7×7 pixels neighboring area centered at location x. $I\left(v\right)$ and $T\left(v\right)$ are the pixels intensities at location v. $\bar{I}$ and $\bar{T}$ are the average pixel intensities of I and T computed at $\Omega\left(x\right)$. Larger value of ZNCC indicates high similarity.

2. Correlation map is now obtained, to reduce noise, Gaussian filter of size 7 pixels is applied. Then, it is converted to binary image with a threshold value (th=0.55 in our experiments);
3. Finally, morphological operation is applied to fill the holes in the binary image.

4. EXPERIMENTAL RESULTS

In this section, the performance of the proposed detection method is evaluated. Section 4.1 describes the test image dataset used in our experiments. Error measures are introduced in section 4.2. Results on MICC-F220 and benchmark datasets are illustrated in section 4.3 and 4.4, respectively. A comparison of the proposed method and other related methods is given in section 4.5. In section 4.6, the robustness

of the proposed method to processing operations is shown. Finally, section 4.7 shows the ability of proposed method to detect multiple copy-move forgeries. All measurements are performed on a desktop computer with Intel Core i5 1.7GHz CPU and 4 GB RAM memory, running Matlab R2016b.

4.1. Test Image Dataset

In our experiments, two publicly available datasets are used. Both are the most widely used datasets by CMFD methods (Bakiah et al., 2016). The first dataset is MICC-F220 introduced by Amerini (Amerini et al., 2011). It totally consists of 220 images: 110 are original images and 110 are tampered. The image resolution ranges from 722 × 480 to 800 × 600 pixels. About 1.2% of the entire image is covered by a forged region. The processing operation in this dataset only limited to translation, scaling and rotation. The ground truth of this dataset is not given. The second dataset used benchmark dataset created by (Christlein et al., 2012). This dataset is consisting of 48 basic images and their transformed images, such as rotation, scaling, JPEG compression and additive noise. Parameters applied on each attack is given in Table 1. Images of this dataset are quite large, its average size is about 3000 × 2300 pixels. About 10% of the entire image is covered by a forged region. In this dataset, the duplicated regions are meaningful, which are categorized as either: rough (e.g., rocks), smooth (e.g., sky), or structured (Christlein et al., 2012). This dataset is provided with a ground truth. Table 2 illustrates the details about each dataset.

In our experiments, totally 1756 images have been tested. There are 220 images from MICC-F220 dataset. From Benchmarking dataset: (1) 48 original images, (2) Plain copy-move: 48 tampered images without any processing operations applied. (3) Rotation: the duplicated regions are rotated by angle varying from 2° to 10° with step length 2°. This means that there are totally 48 × 5 = 240 images. (4) Scaling: the duplicated regions are rescaled with ratio between 91% and 109% of its

Table 1. Setting of attacks parameters

Attacks	Parameters
Rotation	Angle (2°:2°:10°)
Scaling	Ratio (0.91:0.02:1.09)
JPEG Compression	Quality Factor (20:10:100)
Noise addition	Deviation (0.02:0.02:0.1)

Table 2. Details about image datasets used

Dataset	Image Size	Total Images	Processing Operations	Ground Truth
MICC-F220	722 × 480 to 800 × 600	Total: 220 Original 110 Tampered 110	-Translation -Rotation -Scaling (symmetric, asymmetric) -Combined transformation	No
Benchmark CMFD	420 × 300 to 3888×2592	Original 48 Tampered - 48 (plain CMF) -240 (Rotated) -480 (Scaled) -423(JPEG) -240(Noise)	-Rotation -Scaling -JPEG Compression -Noise -Combined transformation	Yes

original size, with step length 2%. That results in 48 × 10 = 480 images. (5) JPEG Compression: The forged images are compressed with quality factors varying from 20 to 100 with step length 20. In this case, there are 84 × 9 = 432 images. (6) Noise addition: noise is added to duplicated regions with standard deviation varying from 0.02 to 0.1 with step length 0.02. Therefore, totally there are 240 images. (7) Multiple Copies: for each of the 48 images, a block size of 64 × 64 pixels are selected and randomly copied five times.

4.2. Error Measures

To test the performance of our CMFD method, we follow the approach presented by (Christlein et al., 2012). Performance of CMFD scheme is evaluated at two levels: (1) Image level: the ability to determine if the image has been tampered or not. (2) Pixel level: the ability to localize tampered regions correctly. Commonly used evaluation metrics in CMFD to calculate the accuracy are True Positive Ratio (TPR) and False Positive Ratio (FPR) see Table 3. A CMFD technique is efficient if it maintains a high TPR while the FPR at the minimum level. The calculation for TPR (recall), FPR and precision given as:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{17}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{18}$$

$$\text{FPR} = \frac{FP}{FP + TN} \tag{19}$$

In the proposed method, if at least one affine transformation is estimated between forged image regions, an image is taken into account as forged. In addition, F1 score is used as an evaluation metric (Christlein et al., 2012), which combines precision and recall into a single value:

$$F_1 = 2 \cdot \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} \tag{20}$$

Table 3. Evaluation measures description

Measures	Description
TP (True positive)	Correctly detected forged images
TN (True Negative)	Correctly detected original images
FP (False positive)	Original images falsely detected as forged
FN (False Negative)	Falsely missed forged images

At pixel level, the same evaluation metrics are used where TP represents number of pixels that are correctly detected as forged, FP number of pixels that are falsely detected as forged and FN shows falsely missed forged pixels.

4.3. Results on MICC-F220 Dataset

It worth to notice that image size and forged region size play an important role when evaluating forgery detection method. In this dataset, image sizes are not so large. As mentioned earlier, images size is varying from 722×480 to 800×600. The forged regions are small compared to the whole image. It was found that the smaller the size of the image and the forged region is, the lesser the number of features and matched points are found. In our matching method, the threshold value is set to 0.5 that yields the best results. Lower threshold value will result in small matched points while larger values will result in high false matches. For the cluster validity measures, both gap statistics and Silhouette width are applied, and the results are compared. The k value (clusters list) is varying from 1 to 7. Large range of k will result in low TPR and high FPR because cluster sizes depend highly on number of matched points. Silhouette width produces the best results in terms of TPR and FPR as illustrated in Table 4.

4.4. Results on Benchmark Dataset

As previously mentioned, the image size of this dataset is relatively large. Its average size is 3000×2300. Large images are more challenging, since an overall higher number of feature vectors exists, and thus there is a higher probability of false positives. In this case, the matching threshold is set to 0.4. To avoid high false positives, the value of k is set from 1 to 20. The ability of the proposed method is examined in different cases: plain copy-move forgery, robustness to processing operations: rotation, scaling, JPEG compression and noise addition and in multiple pasted regions. We also compare results using gap statistics and Silhouette width. In this dataset, gap statistics represent the best results. Figure 5 shows some examples of tampered images detected by the proposed method. The localization detection results on the test images with CMF regions fused in the background are illustrated in Figure 6. The proposed method detects most CMF regions.

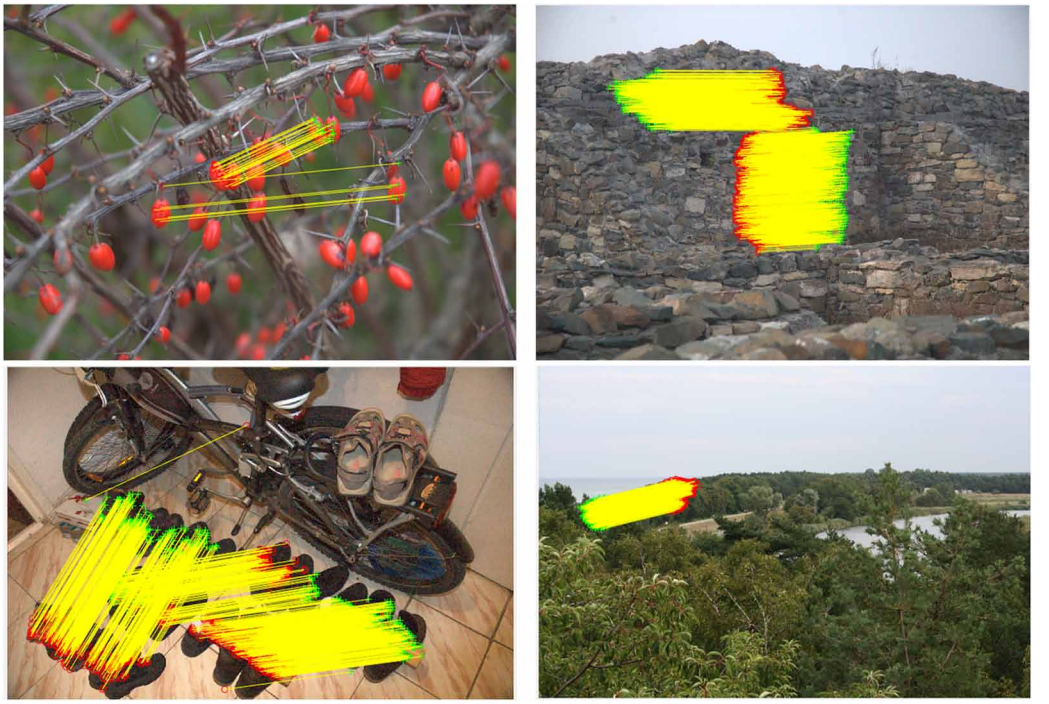
4.5. Comparisons With Other Relevant Methods

To verify the performance of the proposed method, our results is compared with various recent keypoint-based methods. All comparisons are made using MICC-F220 dataset and the benchmark dataset. The methods used for comparison include: pan and Lyu (Pan & Lyu, 2010), Amerirni et. al (Amerini et al., 2011), Shivakumar and Baboo (B.L.Shivakumar & Baboo, 2011), Li et. al (Li et al., 2015), Hashmi et. al (Hashmi et al., 2014), and Yang et al. (Yang et al., 2017). Using MICC-F220 dataset, the proposed method is compared with methods in (Amerini et al., 2011) and (Hashmi et al., 2014). The proposed method and the method presented in (Amerini et al., 2011) achieve best TPR, but the proposed method achieves less FPR as shown in Table 5. The processing time of the proposed method (per image) on average about 0.43 seconds, whereas the other two methods take about 4.94 and 2 seconds respectively. Using benchmarking dataset, the performance in case of plain copy-move forgery is evaluated. In such case, 48 original images and 48 forged images are used without applying any processing operations. In this case, the CMFD methods must differentiate whether the image has

Table 4. TPR and FPR values on MICC-F220 with respect to cluster evaluation method

Method	TPR	FPR
Gap statistics	95.45%	8.18%
Silhouette width	100%	6.36%

Figure 5. Examples of tampered images detected by proposed method



been tampered or not. Detection results of plain copy-move forgery are shown in Table 6. Note that the proposed method and the method presented in (Li et al., 2015) obtain the best results in terms of recall rate, 100% and 97.72%, respectively. For precision rate, the proposed method obtains the best result reaching to 90.9%, followed by the method presented in (Hashmi et al., 2014) of 88.89%. In addition to the precision and recall, the proposed method achieves the best F_1 score of 95.23% compared to other methods. In conclusion, the proposed method obtains the best results in terms of recall, precision and F_1 core compared to other methods.

4.6. Robustness to Processing Operations

The proposed method has additionally been tested in terms of detection performance from a robustness point of view; the impact of rotation, scaling, JPEG compression and noise addition using benchmark dataset (Christlein et al., 2012):

1. **Robustness to gaussian noise:** Image intensities between 0 and 1 are normalized and zero-mean Gaussian noise with standard deviations of 0.02, 0.04, 0.06, 0.08 and 0.10 is added. It can be noticed that as standard deviation increased the false negatives also increased and true positives decreased. In addition, a standard deviation of 0.10 leads to obviously visible artifacts (Christlein et al., 2012). Generally, the proposed method maintains high TPR as illustrated in Table 7;
2. **Robustness to JPEG compression artifacts:** The quality factors varied between 100 and 20 with step length 10. The same JPEG compression applied to 48 forgeries per quality level. The visual quality of the image is highly affected when the quality factor is very low. For real-world forgeries, quality levels down at least 70 are considered as acceptable assumptions (Christlein et al., 2012). TPR tends to slightly reduce when image quality decreases. Proposed method maintains high TPR as illustrated in Table 7;

Figure 6. Detection results on the images with copy-move forgery regions combined in the background. The first column represents the test images from benchmark dataset. The second column represents the ground truth of the copy-move forgery regions in these images. The third column shows the localization detection results of the proposed method.

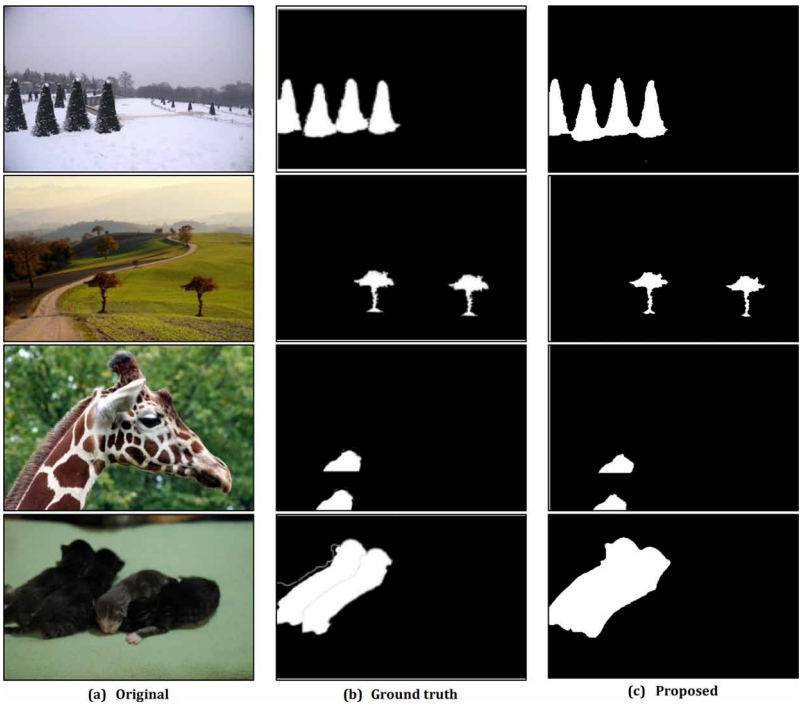


Table 5. Detection results on MICC-F220 dataset and processing time (average, per image)

Method	TPR (%)	FPR (%)	Time (s)
Amerirni et. al (2011)	100	8	4.94
Hashmi et. al (2014)	80	10	2
Proposed	100	6.36	0.43

Table 6. Detection results of the plain copy-move forgery on benchmark dataset

Methods	Precision (%)	Recall (%)	F_1
Pan and Lyu (2010)	80.49	68.75	74.15
Amerirni et. al (2011)	88.4	79.2	79.2
Shivakumar and Baboo (2011)	77.27	70.83	73.90
Li et. al (2014)	70.17	83.33	76.19
Hashmi et. al (2014)	88.89	80	84.21
Yang et. al (2017)	78.33	97.92	87.04
Proposed	90.90	100	95.23

3. **Robustness to rotation and scaling:** Flexibility of CMFD algorithms to affine transformations, like scaling and rotation is very important. The proposed method shows strong invariance to scaling and rotation. Performance of the proposed remains relatively stable across the whole scaling parameters and different rotation angles. Proposed method results in 100% TPR for both scaling and rotation see Table 7.

4.7. Detection of Multiple Copies

In the proposed method, we address the detection of multiple copies of the same region. As more combinations of matched regions, the chance of false match increases. Table 8 illustrates the detection results of our proposed method of multiple copies in terms of TPR using different threshold values. Generally, the performance will decrease, mainly since the random choice of small blocks typically yields regions with only a few matched keypoints (Christlein et al., 2012).

5. CONCLUSION

Detecting copy-move forgery is a challenging task. Dependence of empirical thresholds in existing CMFD techniques is a critical issue. This paper proposes a CMFD method that automatically determines the optimal number of clusters using internal cluster validity measures. The method uses Gap Statistic and Silhouette width for automatic cutoff threshold in AHC. The proposed method has been evaluated using two publicly available datasets MICC-F220 and Benchmark dataset. Experimental results exhibit that the proposed method yields higher precision and recall, and lower false negative values compared to alternative similar works within the literature. It also shows robustness against different attacks such as scaling, rotation, JPEG compression, and additive noise. Future work can be extended to work on videos and handle other types of image forgery like image splicing.

Table 7. Robustness to processing operations

Attacks	Total Number of Images	Parameters	TP	Recall (%)
Rotation (angle)	240	2°	48	100
		4°	48	
		6°	48	
		8°	48	
		10°	48	
Scaling (ratio)	480	0.91	48	100
		0.93	48	
		0.95	48	
		0.97	48	
		0.99	48	
		1.01	48	
		1.03	48	
		1.05	48	
		1.07	48	
		1.09	48	
JPEG Compression (quality factor)	432	20	45	98.61
		30	47	
		40	46	
		50	48	
		60	48	
		70	48	
		80	48	
		90	48	
		100	48	
Noise (standard deviation)	240	0.02	47	96.67
		0.04	47	
		0.06	46	
		0.08	46	
		0.10	46	

Table 8. Results for multiple copy-move forgery

Threshold	TPR (%)
0.4	93.75
0.5	95.83
0.6	97.92

REFERENCES

Abe, R., Miyamoto, S., & Hamasuna, Y. (2017). Hierarchical Clustering Algorithms with Automatic Estimation of The Number of Clusters. *Proceedings of the 17th World Congress of International Fuzzy Systems Association and 9th International Conference on Soft Computing and Intelligent Systems (IFSA-SCIS)* (pp. 1–5). Academic Press. doi:10.1109/IFSA-SCIS.2017.8023241

Al-Qershi, O. M., & Khoo, B. E. (2013). Passive Detection of Copy-Move Forgery in Digital Images: State-Of-The-Art. *Forensic Science International*, *231*(1–3), 284–295. doi:10.1016/j.forsciint.2013.05.027 PMID:23890651

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013). Copy-Move Forgery Detection and Localization by Means of Robust Clustering With J-Linkage. *Signal Processing Image Communication*, *28*(6), 659–669. doi:10.1016/j.image.2013.03.006

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 Transactions on Information Forensics and Security*, *6*(3 Part 2), 1099–1110. doi:10.1109/TIFS.2011.2129512

Bakiah, N., Warif, A., Wahid, A., Wahab, A., Yamani, M., Idris, I., & Shamshirband, S. et al. (2016). Copy-move forgery detection: Survey, challenges and future directions. *Journal of Network and Computer Applications*, *75*, 259–278. doi:10.1016/j.jnca.2016.09.008

Cao, Y., Gao, T., Fan, L., & Yang, Q. (2011a). A Robust Detection Algorithm for Copy-Move Forgery in Digital Images. *Forensic Science International*, *214*(1–3), 33–43. PMID:21813252

Cao, Y., Gao, T., Fan, L., & Yang, Q. (2011b). A Robust Detection Algorithm for Region Duplication in Digital Images. *International Journal of Digital Content Technology and Its Applications*, *5*(6), 95–103. doi:10.4156/jdcta.vol5.issue6.12

Christlein, V., Riess, C., & Angelopoulou, E. (2010). A Study on Features for the Detection of Copy-Move Forgeries. *Sicherheit*, 105–116.

Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An Evaluation of Popular Copy-Move Forgery Detection Approaches. *IEEE Transactions on Information Forensics and Security*, *7*(6), 1841–1854. doi:10.1109/TIFS.2012.2218597

Dada, A., Dharaskar, R. V., & Thakare, V. M. (2016). A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques. *Procedia Computer Science*, *78*, 61–67. doi:10.1016/j.procs.2016.02.011

Everitt, B. S., Landau, S., Leese, M., & Stahl, D. (2011). *Cluster Analysis* (5th ed.). London: Wiley. doi:10.1002/9780470977811

Farid, H. (2006). Exposing Digital Forgeries in Scientific Images. *Proceedings of the 8th Workshop on Multimedia and Security* (pp. 29-36). ACM.

Fischler, M., & Bolles, R. C. (1981). Random Sample Consensus: A paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography. *Communications of the ACM*, *24*(6), 381–395. doi:10.1145/358669.358692

Fridrich, J., Soukal, D., & Lukáš, J. (2003). Detection of Copy-Move Forgery in Digital Images. *Proceedings of the Digital Forensic Research Workshop*. Academic Press.

Gan, G. (2007). *Data Clustering Theory, Algorithms, and Applications* (Vol. 20). Alexandria, Virginia: Siam. doi:10.1137/1.9780898718348

Halkidi, M., Batistakis, Y., & Vazirgiannis, M. (2002). Clustering Validity Checking Methods: Part II. *ACM Special Interest Group on Management of Data*, *31*(3), 40–45.

Hashmi, M. F., Anand, V., & Keskar, A. G. (2014). Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform. *AASRI Procedia*, *9*, 84–91. doi:10.1016/j.aasri.2014.09.015

Hastie, T., Tibshirani, R., & Friedman, J. (2003). The Elements of Statistical Learning Data (2nd ed.). Springer.

Hu, J., Zhang, H., Gao, Q., & Huang, H. (2011). An Improved Lexicographical Sort Algorithm of Copy-Move Forgery Detection. *Proceedings of the 2nd International Conference on Networking and Distributed Computing* (pp. 23–27). Academic Press. doi:10.1109/ICNDC.2011.12

Junhong, Z. (2010). Detection of Copy-Move Forgery Based on One Improved LLE method. *Proceedings of the 2nd International Conference on Advanced Computer Control* (Vol. 4, pp. 547–550). Academic Press. doi:10.1109/ICACC.2010.5486861

Katta, R. M. R., & Patro, C. S. (2017). Influence of Web Attributes on Consumer Purchase Intentions. *International Journal of Sociotechnology and Knowledge Development*, *9*(2), 1–16. doi:10.4018/IJSKD.2017040101

Kumar, R., & Sharma, H. (2008). Comparative Study of CLAHE, DSIHE & DHE Schemes. *International Journal of Research in Management, Science & Technology*, *1*(1), 1–4.

Li, J., Li, X., Yang, B., & Sun, X. (2015). Segmentation-Based Image Copy-Move Forgery Detection Scheme. *IEEE Transactions on Information Forensics and Security*, *10*(3), 507–518. doi:10.1109/TIFS.2014.2381872

Lin, X., Li, J. H., Wang, S. L., Liew, A. W. C., Cheng, F., & Huang, X. S. (2018). Recent Advances in Passive Digital Image Security Forensics: A Brief Review. *Engineering*, *4*(1), 29–39. doi:10.1016/j.eng.2018.02.008

Liu, G., Wang, J., Lian, S., & Wang, Z. (2010). A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications*, *34*(5), 1557–1565. doi:10.1016/j.jnca.2010.09.001

Lowe, D. G. (2004). Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision*, *60*(2), 91–110. doi:10.1023/B:VISI.0000029664.99615.94

Ma, J., Fan, X., Yang, S. X., Zhang, X., & Zhu, X. (2017). Contrast Limited Adaptive Histogram Equalization Based Fusion for Underwater Image Enhancement.

Mahajan, P., Delhi, N., & Rana, A. (2018). Sentiment Classification-How to Quantify Public Emotions Using Twitter. *International Journal of Sociotechnology and Knowledge Development*, *10*(1), 57–71. doi:10.4018/IJSKD.2018010104

Mohamdian, Z., & Pouyan, A. A. (2013). Detection of Duplication Forgery in Digital Images in Uniform and Non-Uniform Regions. *Proceedings of the 15th International Conference on Computer Modelling and Simulation* (Vol. 1, pp. 455–460). Academic Press. doi:10.1109/UKSim.2013.94

Muja, M., & Lowe, D. G. (2009). Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration. *Proceedings of the VISAPP International Conference on Computer Vision Theory and Applications* (Vol. 1, pp. 331–340). Academic Press.

Muliawaty, L., Alamsyah, K., Salamah, U., & Maylawati, D. S. (2019). The Concept of Big Data in Bureaucratic Service Using Sentiment Analysis. *International Journal of Sociotechnology and Knowledge Development*, *11*(3), 13. doi:10.4018/IJSKD.2019070101

Pan, X., & Lyu, S. (2010). Region Duplication Detection Using Image Feature Matching. *IEEE Transactions on Information Forensics and Security*, *5*(4), 857–867. doi:10.1109/TIFS.2010.2078506

Qureshi, M. A., & Deriche, M. (2015). A Bibliography of Pixel-Based Blind Image Forgery Detection Techniques. *Signal Processing: Image Communication, 39*(Part A), 46-74.

Redi, J. A., Taktak, W., & Dugelay, J. (2011). Digital Image Forensics: A Booklet for Beginners. *Multimedia Tools and Applications*, *51*(1), 133–162. doi:10.1007/s11042-010-0620-1

Sharma, S., & Ghanekar, U. (2019). Spliced Image Classification and Tampered Region Localization Using Local Directional Pattern. *International Journal of Image, Graphics and Signal Processing*, *11*(3), 35–42. doi:10.5815/ijigsp.2019.03.05

Shivakumar, B. L., & Baboo, S. (2011). Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors. *International Journal of Computers and Applications*, *27*(3), 9–17. doi:10.5120/3283-4472

Tibshirani, R., Walther, G., & Hastie, T. (2001). Estimating the Number of Clusters in A Data Set Via the Gap Statistic. *Journal of the Royal Statistical Society. Series A, (Statistics in Society)*, *63*(2), 411–423. doi:10.1111/1467-9868.00293

Tijdink, J. K., Verbeke, R., & Smulders, Y. M. (2014). Publication Pressure and Scientific Misconduct in Medical Scientists. *Journal of Empirical Research on Human Research Ethics*, *9*(5), 64–71. doi:10.1177/1556264614552421 PMID:25747691

Walia, S., & Kumar, K. (2018). An Eagle-Eye View of Recent Digital Image Forgery Detection Methods. *Proceedings of the International Conference on Next Generation Computing Technologies* (pp. 469–487). Academic Press. doi:10.1007/978-981-10-8660-1_36

Yang, F., Li, J., Lu, W., & Weng, J. (2017). Copy-Move Forgery Detection Based on Hybrid Features. *Engineering Applications of Artificial Intelligence*, *59*, 73–83. doi:10.1016/j.engappai.2016.12.022

Aya Hegazi is a teaching assistant at faculty of computers and informatics, Benha University.

Ahmed Taha received his M.Sc. degree and his Ph.D. degree in computer science, at Ain Shams University, Egypt, in February 2009 and July 2015 respectively. He currently works as assistant professor at computer science department, Benha University, Egypt. His research interests are: computer vision and image processing (human behavior analysis - video surveillance systems), digital forensics (image forgery detection – document forgery detection), security (encryption – steganography – cloud computing), content-based retrieval (Arabic text retrieval - video scenes classification-video scenes retrieval – trademark image retrieval - closed-caption technology).

Mazen M. Selim received the BSc in Electrical Engineering in 1982, the MSc in 1987 and PhD in 1993 from Zagazig University (Benha Branch) in electrical and communication engineering. He is now a Professor at the faculty of computers and informatics, Benha University. His areas of interest are image processing, biometrics, sign language, content-based image retrieval (CBIR), face recognition, and watermarking.