KEYPOINT BASED AUTHENTICATION AND LOCALIZATION OF COPY-MOVE FORGERY IN DIGITAL IMAGE

Somayeh Sadeghi[1], Hamid A. Jalab[2], KokSheik Wong[3], Diaa Uliyan[4], Sajjad Dadkhah[5]

[1, 2 ,3, 4] Faculty of Computer Science and Information Technology, University of Malaya,
Kuala Lumpur, Malaysia
[5] Faculty of Computing, University Technology Malaysia
Kuala Lumpur, Malaysia

Email: ssomayeh@siswa.um.edu.my[1], hamidjalab@um.edu.my[2], koksheik@um.edu.my[3],
diaa_uliyan@siswa.um.edu.my[4], dsajjad2@live.utm.my[5]

ABSTRACT

With the development of powerful image processing tools and the increasing trend of using images as the main carrier of information, digital image forgery has become an increasingly serious issue. In copy-move forgery, one part of an image is copied and placed elsewhere in the same image. This paper puts forward an effective method based on SIFT for detecting copy-move forgery in digital image. The proposed method can accurately authenticate digital image and locate areas which have been tampered with. The algorithm starts by using scale-invariant features transform (SIFT) to extract local image features, which are known as keypoints, and then searches for similar keypoints based on their Euclidean distances. Finally, the matched keypoints, which represent the copied and pasted areas, are associated with one and another to indicate which parts of the image have been tampered with. Experiments are performed to validate the effectiveness of this method on different attacks, and to quantify its robustness against post-processing. Results show that the method is robust against several geometric processings, including JPEG compression, rotation, noise, and scaling. As a representative result, when considering the standard test dataset MICC-F220, the proposed method achieves true and false positive rates of 100% and 3.12%, respectively.

Keywords: Digital Forensic, Copy-move Forgery detection, Passive Authentication, Duplicated Detection

1.0 INTRODUCTION

In recent years, the number of criminal cases making use of digital media has steadily increased, hand-in-hand with the continual innovation of software technologies. As digital media is becoming an ever-more integral part of daily life, digital image, audio, and video are increasingly being presented in courts of law as evidence of criminal activity or wrongdoing [1]. However, the authenticity of a given digital image has become more difficult to validate, as a consequence of the drastic changes in the production, editing and dissemination of digital image.

In the last decade, researchers in digital image forensics have developed various image authentication techniques, with a particular focus on forgery detection. Image forgery detection refers to the authentication of an image and the localization of tampered areas. One of the most important categories of image forgery detection is passive detection, which refers to an authentication process that only considers the features of the image itself, without the need of any additional information. Passive digital image forgery detection can be further classified into three categories:

i. **Image splicing** is the process of creating a fake image by cutting out a portion of one image and pasting it into a different image [2, 3].
ii. **Image retouching** is not a direct alteration of an image, but the enhancement of a few features of an image. Thus, this process can be considered as a less damaging type of digital image forgery, and it is a common practice among magazine photo editors [4, 5].
iii. **Copy-move forgery** covers one region of an image by another selected region from the same image [6]. This technique is widely utilized for illegal purposes, in order to conceal or emphasize certain image details by cloning an area of an image to a different area [7-9]. This type of forgery has become

notorious, as its detection requires greater technical skills. It is because the source and destination of the forged image are the same. This paper focuses on this category of forgery.

One of the earliest examples of image forgery is shown in Fig.1, a photo of Queen Elizabeth and the former Canadian prime minister William Lyon Mackenzie King taken in Banff, Alberta in 1939. King George VI was eliminated from the original image and the tampered image was used for the prime minister's election campaign. Some hypothesized that the image was manipulated by the prime minister to show his power with a photo of only him and the Queen [10].

(a) Doctored image (b) Original Image

Fig 1.One of the earliest forged images [9].

Although the original (i.e., source) region is not altered but simply copied and pasted onto another region in the same image when performing copy-move forgery, the process can be further complicated by applying image processing techniques such as blurring, rotation, or scaling, to the region of interest. Conventional detection methods lack the robustness against such image processing techniques, which are also considered as attacks from the perspective of copy-move forgery [8]. However, the application of image processing techniques makes the authentication of digital images and the localization of tampered regions more technically challenging. In addition to the robustness of the detection algorithm, the computational time needed is also an important issue, given the vast number of images that are ubiquitously available nowadays.

Therefore, this paper puts forward a detection and localization method for copy-move forgery based on scale-invariant features transform (SIFT) [11] and feature-matching. Although a number of copy-move forgery detection methods are already in existence [8, 12-18], the proposed detection method demonstrates an improvement in detection rate, and it is more robust against noise, rotation, scale, as well as JPEG compression. The proposed method, which is based on SIFT, can authenticate a digital image while locating the tampered areas, if there are any. SIFT is chosen because its extracted local features which are invariant to rotation, scale, and illumination change of the image. These features are also unique, informative, and robust against noise [19]. Our work makes the following contributions: (a) descriptors are clustered using a centroid linkage method to improve detection accuracy; (b) a second-level post-processing of filtering is proposed to improve the true positive and false positive rates (Step 7 of the proposed method).

The rest of the paper is structured as follows: Section 2 discusses then conventional copy-move forgery detection methods. Section 3 details the proposed forgery detection method. Section 4 presents the experimental results of forgery detection. Lastly, conclusions are drawn in Section 5.

2.0 RELATED WORK

As mentioned earlier, copy-move forgery is the process of duplicating one part of an image and pasting it to another part of the same image. Various copy-move forgery detection methods have been proposed to solve the problems related to image authentication. These methods can be categorized into block generation and keypoint-based methods, which are further discussed in the following subsections.

2.1 Block Generation-based Methods

In block generation-based methods, a suspicious image is segmented into overlapping blocks of uniform size. If the size of each block is $\mathrm{b} \times \mathrm{b}$ pixels, then there are $(\mathrm{M} - \mathrm{b} + 1) \times (\mathrm{N} - \mathrm{b} + 1)$ blocks, where $M \times N$ represents the image dimensions for $b < \min\{M, N\}$. Then, a feature vector is computed for each block, either by singular value decomposition (SVD), discrete wavelet transformation (DWT), or Fourier-Mellin transformation [20, 21]. The feature vectors are then sorted, and similar feature vectors are subsequently matched with one another. The majority of conventional methods utilize lexicographic sorting to identify similar feature vectors. The location of the copy-pasted area is also identified, or in other words, localized. Finally, a detection area map is obtained.

In most conventional techniques, the blocks are represented in a concise way to enhance robustness and reduce computational complexity. However, these methods are time-consuming, because the features are extracted from millions of blocks and then sorted. Najah et al. proposed an efficient, non-intrusive method based on dyadic wavelet transformation [22]. In this method, a separate noise image is created based on the noise pattern of each sub-block, which are then collectively utilized to approximate the total noise of the image. To complete the process, blocks with similar noise histograms are marked as potentially copy-pasted areas. However, this method can detect forgeries only when the image has a simple background.

Huang et al. [23] presented a detection technique based on discrete cosine transformation (DCT). They improved upon Fridrich et al.'s DCT-based method [8] by reducing the rate of false matches. A lexicographical sorting algorithm based on distance was proposed to improve matching accuracy. It is robust against noise addition and blurring, but not against rotation.

Hou et al. [24] proposed a new algorithm that uses phase correlation within an image to detect and locate copy-move forgery. This algorithm can detect small tampered areas with low computational complexity, because it uses a larger overlap ratio (which is the percentage of overlapping regions of the sub-images). Nonetheless, the detection performance of this method drops when the copy-move region lies in two or more sub-images.

Cao et al. [25] proposed a DCT-based method that has a lower computational complexity than the conventional methods [7,13,20] because the dimension of the feature vector is reduced. Specifically, DCT is applied to each image block to generate quantized coefficients for extracting useful features from each block. Similar blocks are identified, and the duplicated image blocks are matched according to a pre-set threshold value.

2.2 Keypoint-based Methods

Several detection methods based on image keypoint-matching (e.g. SIFT) have recently been proposed for locating copy-pasted areas [12, 16]. Unlike block generation-based methods, keypoint-based methods consider features extracted from the entire image (i.e., without subdivision), and the extracted features are compared with one and another to locate similar keypoints [26]. The feature vector for each keypoint is then extracted, and similar features within the image are subsequently matched. The main advantage of keypoint-based method over

block generation-based method is its low computational complexity, which is due to its low post-processing operation.

Amerini et al. [15] proposed a novel forgery detection method based on SIFT. When compared with previous methods proposed by Fridrich et al. [8] and Popescu et al. [17], the computational time, true positive rate, and false positive rate of this SIFT-based method were all improved. In a related approach [27], the grey-level feature is combined with the SIFT features to form a new feature vector. This approach successfully reduced false matching rate, but at the expense of greater time complexity.

Lin and Wu [28] proposed a copy-move forgery detection based on Speeded-up Robust Features (SURF) and DCT. The detection was accomplished by analysing the double compression effect in the spatial and DCT domains. The features were extracted using a SURF descriptor, so that the algorithm would be robust against rotation and scaling.

Although numerous copy-move forgery detection methods have been proposed, they are still hindered by several drawbacks, including low localization accuracy and high computational cost. For example, Shen et al.'s method [27] is robust against Gaussian blurring and its false matching rate is lower than that of conventional methods. However, their method has a high time complexity because the SIFT and grey level features must be extracted together. Bo et al. [29] proposed a copy-move forgery detection method based on SURF descriptors. This method is robust against rotation and scaling, but its computational time is high. In addition, only visual-based results were included in their results without quantitative measurements.

The majority of the aforementioned conventional methods are either not robust against all post-processing operations or have a high computational time. To overcome the robustness issues while maintaining the low computational time, we propose a novel copy-move forgery detection method based on SIFT. SIFT is utilized to extract features from a suspicious image, which is then followed by the clustering of the descriptors and the use of a second level of filtering to suppress false matches.

3.0 PROPOSED COPY-MOVE FORGERY DETECTION ALGORITHM

In this section, we propose a method based on SIFT for the authentication and localization of copy-moved areas in an image. There are various feature extraction techniques available such as corner detection, edge detection [30], etc., but SIFT is chosen in this work for feature extraction because of its robustness against scale, rotation, blur and change in illumination. Although SURF and principal component analysis (PCA)-SIFT are also robust against image transformations, there are some drawbacks. Specifically, the authors in [11, 31] proposed a technique based on PCA to control gradient patches instead of histograms. They proved that PCA-based descriptors are robust to image manipulation, but the execution time for feature extraction is very slow [31]. Later in 2006, Bay et al. [32] proposed SURF, which used integral images for image convolutions and a Fast-Hessian detector. It works faster than the SIFT and PCA techniques, but in terms of robustness, which is very important for forgery detector, SIFT has better performance.

Fig. 2 illustrates the processes involved in the proposed detection algorithm. First, SIFT is applied to the suspicious image for extraction of the SIFT keypoints. The keypoint descriptors are first extracted and clustered, and then compared with one and another to identify identical areas in the case of copy-move forgery. The detailed procedures are summarized in the following steps:

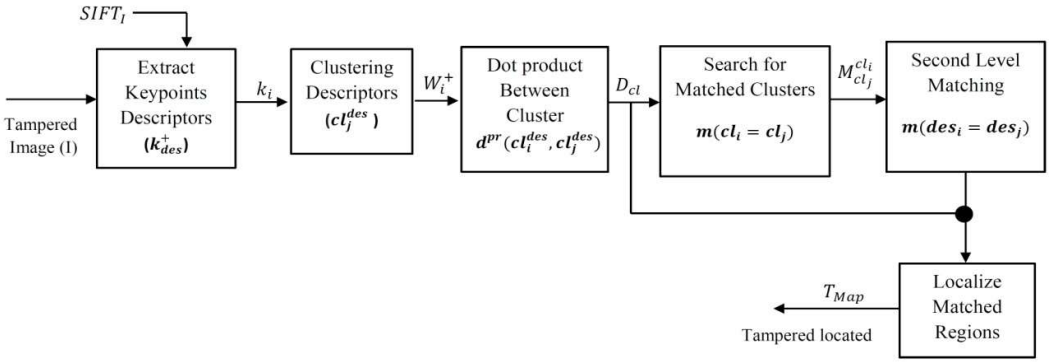

Fig 2. Process flow of the proposed detection method

Step 1. If the input is a colour image, it is converted into grayscale using $\mathrm{I} = 0.299\mathrm{R} + 0.587\mathrm{G} + 0.114\mathrm{B}$ [33].

Step 2. SIFT features are extracted following the procedure below:

Scale-space extrema detection - In the initial step of SIFT, several octaves of the image are generated, and in each octave, images are gradually blurred using the Gaussian Blur operator. Keypoints are generated by checking every two consecutive images in all octaves. The scale-space of the input image is $\mathrm{I}(\mathrm{x},\mathrm{y})$.

$$\mathrm{L}(\mathrm{x},\mathrm{y},\sigma) = \mathrm{G}(\mathrm{x},\mathrm{y},\sigma) * \mathrm{I}(\mathrm{x},\mathrm{y}) \tag{1}$$

where * is the convolution operator in x and y. The Gaussian function is computed using the following expression:

$$\mathrm{G}(\mathrm{x},\mathrm{y},\sigma) = \frac{1}{2\pi\mathrm{e}^2}\mathrm{e}^{\frac{\mathrm{x}_2+\mathrm{y}_2}{\sigma^2}}, \tag{2}$$

where σ is the factor of scale-space. The scale-space extrema in the Difference-of-Gaussian (DoG) function is utilized to improve the robustness of potential interest points against scale and orientation.

i. **Keypoint localization -** Interesting keypoints are identified by computing the maxima and minima in the DoG images. Keypoints are rejected if they have a low contrast or if they are located on an edge.

ii. **Orientation assignment -** An orientation is assigned to each keypoint based on the local image gradient directions to make each keypoint invariant to rotation. The gradient magnitude for the image I(x,y) is computed by:

$$\mathrm{m}(\mathrm{x},\mathrm{y}) = \sqrt{\mathrm{I}_1^2 + \mathrm{I}_2^2}\,, \theta(\mathrm{x},\mathrm{y}) = \arctan(\tfrac{\mathrm{I}_2}{\mathrm{I}_1}), \tag{3}$$

where $\mathrm{m}(\mathrm{x},\mathrm{y})$ is the gradient magnitude, $\mathrm{I}_1 = \mathrm{I}(\mathrm{x}+1,\mathrm{y},\sigma) - \mathrm{I}(\mathrm{x}-1,\mathrm{y},\sigma)$, $\mathrm{I}_2 = \mathrm{I}(\mathrm{x},\mathrm{y}+1,\sigma) - \mathrm{I}(\mathrm{x},\mathrm{y}-1,\sigma)$, and $\theta(\mathrm{x},\mathrm{y})$ is the orientation.

iii. **Generation of keypoint descriptors -** A descriptor is computed for the local image region, which makes the descriptors robust against other possible variations, such as illumination. Keypoints that are robust against local geometrical distortion, scale, noise, and rotation are selected.

Step 3. Descriptors extracted from the image consist of coordinate, scale, and orientation values. Here, the Euclidean distance is computed among the coordinates of the descriptors for identifying which descriptors have greater similarities to one another. Specifically, it is computed by

$$\|a - b\|_2 = \sqrt{\sum_i (a_i - b_i)^2}, \tag{4}$$

where a and b are the coordinates of two descriptors.

Step 4. An agglomerative hierarchical tree clustering method is utilized to group the distance values. Several linkage methods were proposed, including single, centroid and ward's linkage. Their performances are evaluated and the linkage method that works best for the proposed method is selected. Based on our experiments, centroid yields the best performance when compared to the other two methods. It is because centroid uses the Euclidean distance between the centroids of the two clusters, which increase the probability of finding the most similar clusters. We employ the centroid linkage that utilized the Euclidean distance between the centroids of two clusters. If e and f are two clusters, then the centroid linkage is computed as:

$$d(e, f) = P\overline{x_e} - \overline{x_f}p_2, \tag{5}$$

where $\overline{x_e}$ and $\overline{x_f}$ are defined as:

$$\overline{x_e} = \frac{1}{n_e}\sum_{i=1}^{n_e} x_i \ , \overline{x_f} = \frac{1}{n_f}\sum_{i=1}^{n_f} x_j, \tag{6}$$

where $\overline{x_e}$ and $\overline{x_f}$ are the weighted centroids of two other clusters i and j. The number of clusters is empirically defined as 100 to achieve the best result. When the number of clusters is less than 100, more false matches are obtained. When the number of clusters exceeds 100, the resulting matches would be less than the actual number of matches.

Step 5. A search for similar clusters is instigated for grouping purposes. Each cluster is compared with the rest of the clusters to find its match. If a and b are two clusters, the descriptors' coordinates are utilized to compute the dot product, then the angle of the nearest neighbour is checked to see whether it is less than the threshold of 0.5. This process is iterated for all clusters to find all matched clusters. This condition is computed by

$$cd_1 . cd_2 = \|cd_1\| \times \|cd_2\| \times \cos(\theta) \tag{7}$$

where cd_1 and cd_2 are two cluster descriptors and θ is the angle between them. This process is repeated until all clusters are checked against one and another. The adjustment of the threshold value is further explained in section 3.1.

Step 6. Self-matching elimination: Matches between objects that are similar but not copied are deleted. The Euclidean distance between the coordinates of the matched clusters are computed. If the distance is greater than the specified threshold, then those two clusters are matched. The Euclidean distance is computed by using the following:

$$\|cm_1 - cm_2\|_2 = \sqrt{\sum_i (cm_i - cm_i)^2}, \quad (8)$$

where cm_1 and cm_2 are the coordinates of two matched clusters.

Step 7. Second-level matching: If the numbers of detected matched points are less than five, dot products are computed among the descriptors themselves as follows:

$$d_1 . d_2 = \|d_1\| \times \|d_2\| \times \cos\theta \quad (9)$$

where $d_1$and d_2 are descriptors and θ is the angle between d_1 and d_2. This process is repeated until all descriptors are checked with one and another.

Step 8. Descriptor matching: The matching condition is applied to check each value against the rest, in order to discover if two specific descriptors are matched. If the value of the dot product of the first descriptor is greater than that of the second descriptor scaled by the threshold value of 0.255, then those two descriptors are termed as matched. Threshold adjustment is further discussed in Section 3.1.

Step 9. Self-matching elimination: Objects that are similar but not copied are eliminated by computing the Euclidean distance between the coordinates of the matched descriptors. If the distance exceeds the predefined value, then those two descriptors are not matched. Otherwise, these two descriptors are termed the matched pairs, and their coordinates are saved for the next step to locate the tampered regions. The Euclidean distance is calculated using Eq. (8) by replacing cm_l by dm_l, where dm_l are the coordinates of the two matched descriptors for $i = 1$ and 2.

Step 10. Locating duplicated regions: Two output results are generated to locate the duplicated regions in the image. The first output shows the matched points pertaining to cluster matching, and the second output displays the detected areas inferred from descriptor matching. A line connecting the coordinates of similar clusters or descriptors is drawn to indicate the tampered areas. Detection results are shown in Section 4.

As shown in Fig. 3, the procedure commences by converting the image to grayscale and applying SIFT to the output. Similar descriptors (i.e., derived from SIFT) are searched for, and their locations are connected to indicate the tampered regions, if there are any.

```
read IT ← Tampered image
ITG ← R(0.299) + G(0.587) + B(0.114)
SIFT(ITG) ← im + des + loc
Y ← arry ∈ pdist(loc)
Z ← arry ∈ Link(Y)
T ← arry ∈ Clust(Z)
Process
 for all i ∈ Max_T
     for all j ∈ Max_T do
         dpr (T_i × T_j = ||T_i|| × ||T_j|| × cos θ)
         Val_i^dpr < des^ratio(0.5) × Val_j^dpr
     end for
end for
Set m to 0
 if m > 0 then
         for all i ∈ {val} do
             if pdist(loc_i) ; pdist(m_i) > 20 then
                 m_i = 1
             else
                 m_i = 0
             end if
         end for
 end if
 if m < 4 then
         dpr (des_i × des_j = ||des_i|| × ||des_j|| × cos θ)
         Val_i^dpr < des^ratio(0.255) × Val_j^dpr
 end if
          if pdist(loc_i) ; pdist(m_i) > 1 then
              m_i = 1
          else
              m_i = 0
          end if
 line (loc_i, loc_m)
end Process
```

Fig. 3 Pseudo code for the proposed copy-move forgery detection algorithm

3.1 Adjusting Threshold Value

The proposed method is analysed to determine the thresholds for attaining the highest true positive rate (TPR) and lowest false positive rate (FPR) scores. Specifically, the threshold value affects the number of matched keypoints. Several pairs of threshold values are tested to gauge their influences on the identification of the forged and original images. A proper threshold is therefore required to reduce the number of false matches. The goal is to maximise the TPR value while suppressing FPR. The best FPR is the lowest value which means only a few percentage of the original images are incorrectly recognized as forged ones, while the best TPR is the highest value which means all the forged images are correctly recognized as forged.

Table 1 illustrates that the best threshold T values are empirically found to be 0.255 and 0.5 for the first and second comparison conditions, respectively. This table presents the results of threshold analysis for the MICC-F220 image dataset. The best FPR for this dataset is 3.12% and the best TPR is 100%, which is the highest possible TPR value. The reason behind the low FPR in our proposed algorithm is due the judiciously decided threshold value (i.e., 255) for descriptor matching, which contributed in the reduction of the FPR value. Moreover, by employing the centroid clustering method and applying the second level of matching (viz. Step 7), the number of false matches is suppressed and hence the value of FPR is reduced to 3.12%. Also, another possible reason is that the features extracted by SIFT are robust against scale, rotation, blur and Illumination, which further reduce the FPR.

Table.1 Performance in terms of TPR and FPR for various pairs of threshold values

First Threshold	Second Threshold	TPR (%)	FPR (%)
0.3	0.1	24.5	2.1
	0.2	25	7
	0.25	69	7.4
	0.255	81.8	18.1
	0.3	89	11
	0.4	80	9.9
0.4	0.1	63.6	36.6
	0.2	77.3	18.4
	0.25	90.1	7.4
	0.255	95	5
	0.3	91	7.3
	0.4	80	7.9
0.5	0.1	98.3	6.1
	0.2	99.3	5.6
	0.25	100	3.3
	0.255	**100**	**3.1**
	0.3	100	7
	0.4	91	9
0.6	0.1	48	36.5
	0.2	52.4	33
	0.25	41.4	40
	0.255	32.4	20
	0.3	26.8	32.3
	0.4	17	9

The different values of the thresholds for the first and second comparison conditions also have similar influence on the result of TPR and FPR for other datasets (MICC-F2000, MICCF8multi), and we omit the discussion here.

4.0 EXPERIMENTS

We evaluate the performance of the proposed method in terms of image authenticity and forgery detection as well as its localization capability. Here, we provide evidence about the effectiveness of our method, both in terms of detection and localization, on the MICC-F220 and MICC-F2000 datasets. All experiments are performed using a personal computer with 4.0 GHz Intel Pentium processor and 4 GB of RAM.

4.1 Data Collection

Experiment results are collected using two different datasets, namely MICC-F220 and MICC-F2000 [15], which are commonly considered in the literature. These datasets contain images with various contents originating from the Columbia photographic image repository [34] and the author's personal collection. Specifically, MICC-F220 consists of 220 images, of which 110 are original and 110 are tampered images. The resolution of these images ranges from 722 × 480 to 800 × 600 pixels, and the average size of the forged patch covers 1.2% of the entire image. In this dataset, the forged images are created by randomly selecting an image area and duplicating it over

the image by applying various attacks, such as rotation, additive noise, scaling, JPEG compression, or any combination thereof. The attacked area can be square or rectangular in shape.

Meanwhile, MICC-F2000 is a large dataset consisting of 2000 images, each of which has a resolution of 2048×1536 pixels. Among these images, 1300 are original and 700 are tampered. The altered images are generated by implementing 14 types of attack, including noise, scaling, rotation, translation, or any combination thereof. The average size of the forged patch covers 1.12% of the entire image [15]. Tables 2 and 3 summarize the geometrical transformations for the attacks deployed in the MICC-F220 dataset (i.e., 10 attacks, from A to J), and MICC-F2000 dataset (i.e., 14 attacks, from *a* to *o*), respectively. Here, θ refers to the degree of rotation, S_x and S_y are the scaling factors applied to the horizontal and vertical directions of the tampered image, respectively [15].

Table 2. Attacks deployed in the MICC-F220 dataset

Attack	$\theta^{\dagger}$	S_x	S_y
A	0	1	1
B	10	1	1
C	20	1	1
D	30	1	1
E	40	1	1
F	0	1.2	1.2
G	0	1.3	1.3
H	0	1.4	1.2
I	10	1.2	1.2
J	20	1.4	1.2

Table 3. Attacks deployed in the MICC-F2000 dataset

Attack	$\theta^{\dagger}$	S_x	S_y
a	0	1	1
b	0	0.5	0.5
c	0	0.7	0.7
d	0	1.2	1.2
e	0	1.6	1.6
f	0	2	2
g	0	1.6	1
h	0	1.2	1.6
i	5	1	1
j	30	1	1
l	70	1	1
m	90	1	0.6
n	40	1.1	1.6
o	30	0.7	0.9

4.2 Performance Evaluation

To evaluate the sensitivity and robustness of the proposed method, the detection performance is measured in terms of TPR and FPR. These measures are expressed as Eqs. (11) and (12), respectively:

$$\text{TPR} = \frac{\text{\# forged images detected as forged}}{\text{\# forged images}} \tag{11}$$

and

$$\text{FPR} = \frac{\text{\# original images detected as forged}}{\text{\# original images}}, \tag{12}$$

where TPR is the fraction of forged images that are correctly recognized as forged, whereas FPR is the fraction of original images that are incorrectly recognized as forged [15, 18].

As explained previously, our method detects an image as forged if there are at least two keypoints that matched together. The best copy-move forgery detection method would have TPR=100% and FPR = 0%, which means there would be no false positives and no false negatives. The proposed method was evaluated and the value of TPR was found to be 100% and FPR was found to be 3.12%, outperforming all conventional methods considered.

4.3 Qualitative Analysis

To qualitatively evaluate the performance of the proposed method, different experiments are conducted for simple or advanced copy-move forgeries. The shapes of the copied areas are varied by applying different attacks on the original images. There are various attacks which may affect the forgery detection performance, such as JPEG compression, scale, noise or rotation. The following subsections illustrate the accuracy of the proposed method in locating forged areas in the image.

4.4 Multiple Copied Areas

Detecting forgeries in cases of multiple cloning is important, because multiple parts of the original image are changed. Here, we examine the viability of the proposed technique on the MICC-F8 multi-dataset, which consists of eight tampered images with different duplicates of the same area on high-resolution images (dimensions range from 800×532 pixels to 2048×1536 pixels). It is worth mentioning that these images are derived from the MICC-F220 dataset [15]. For the images in MICC-F8, multiple areas are copied and pasted to other parts of the same image to create a forged image. Fig. 4 illustrates examples of test images and their corresponding detected forged areas.

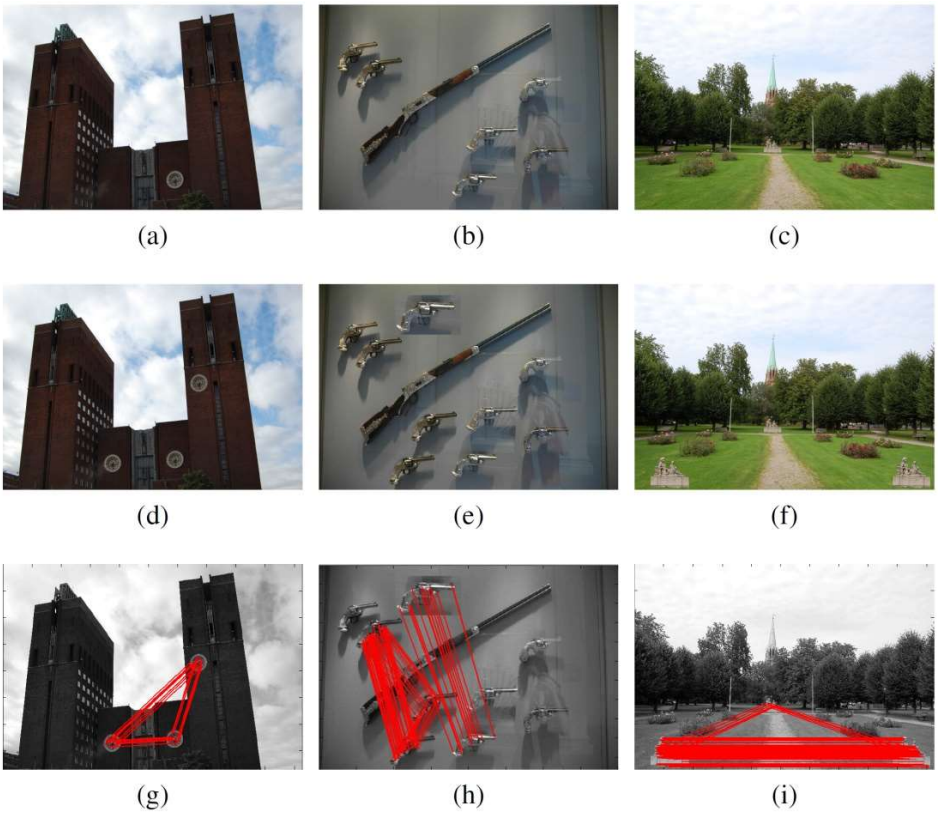

Fig. 4. (a, b, c) The original images, (d, e, f) The forged images, (g, h, i) Detection Results

4.5 Robustness Against Scale, Noise, Rotation and Blurring

Copy-pasted areas are frequently adjusted by further applications of image processing techniques. Here, the tested images are obtained from the MICC-F220 dataset [15]. Fig. 5 illustrates different attacks, including scaling and noise addition, on the original images. Specifically, Fig. 5(a) and (b) show some tampered images which have undergone scaling and Gaussian noise addition attacks, respectively. The corresponding detection results are illustrated in Fig. 5(c) and (d). Results suggest that the proposed detection method can identify and localize the forged areas.

In addition to robustness against noise addition and scaling, the proposed method is also robust against rotation and blurring attacks. A practical forgery detection method should detect tampered regions even under various attacks, including blurring, scaling, or rotation. Figs. 6(a) and (b) show the some tampered images that have undergone rotation and blurring attacks, respectively, and the detection results are correspondingly illustrated in Figs. 6(c) and (d). The proposed method can still identify and localize the forged areas, even after post-processing.

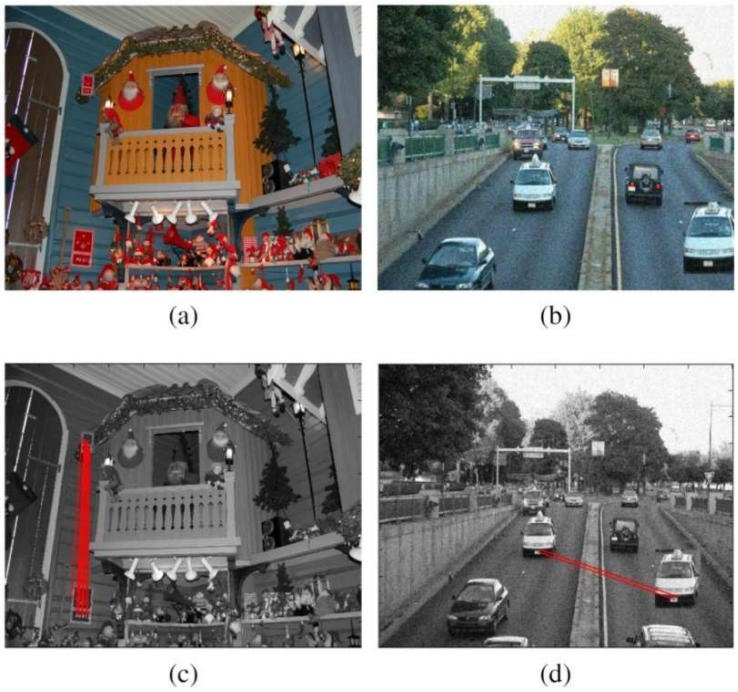

Fig. 5. (a) The tampered image under scale attack, (b) The tampered image under noise attack, (c) Detection result of scaling attack, and (d) Detection result of noise addition attack

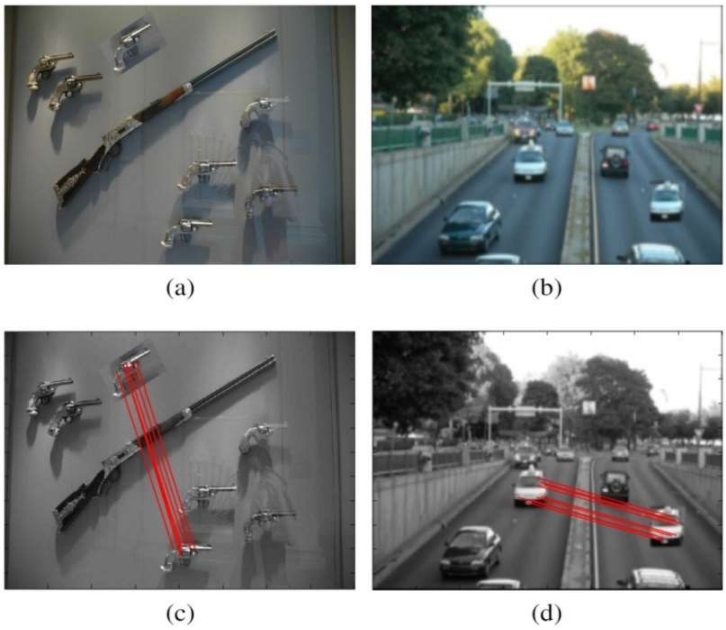

Fig. 6. (a) The tampered image after rotation attack, (b) The tampered image after blurring attack, (c) Detection result of rotation attack, and (d) Detection result of blurring attack

4.6 JPEG Compression Robustness

The majority of images are available in JPEG compressed format. Thus, there is a need to evaluate the performance of the proposed method against JPEG compression. For testing purposes, the test images are compressed using various quality factors Q for

$$Q \in \{5,10,20,50,60,75,80,85,90,95,100\} \quad (13)$$

Fig. 7 illustrates the results of tamper detection for a forged image that has been compressed by various quality factors (Fig 7: (b) Q = 5, (c) Q = 10, (d) Q = 20, (e) Q = 50, (f) Q = 75, (g) Q = 85, (h) Q = 95, (i) Q = 100). Experiment results show that the proposed method is robustness against JPEG compression attacks. Notably, the detection rate is still satisfactory even when the compression ratio is high (e.g., Q < 50).

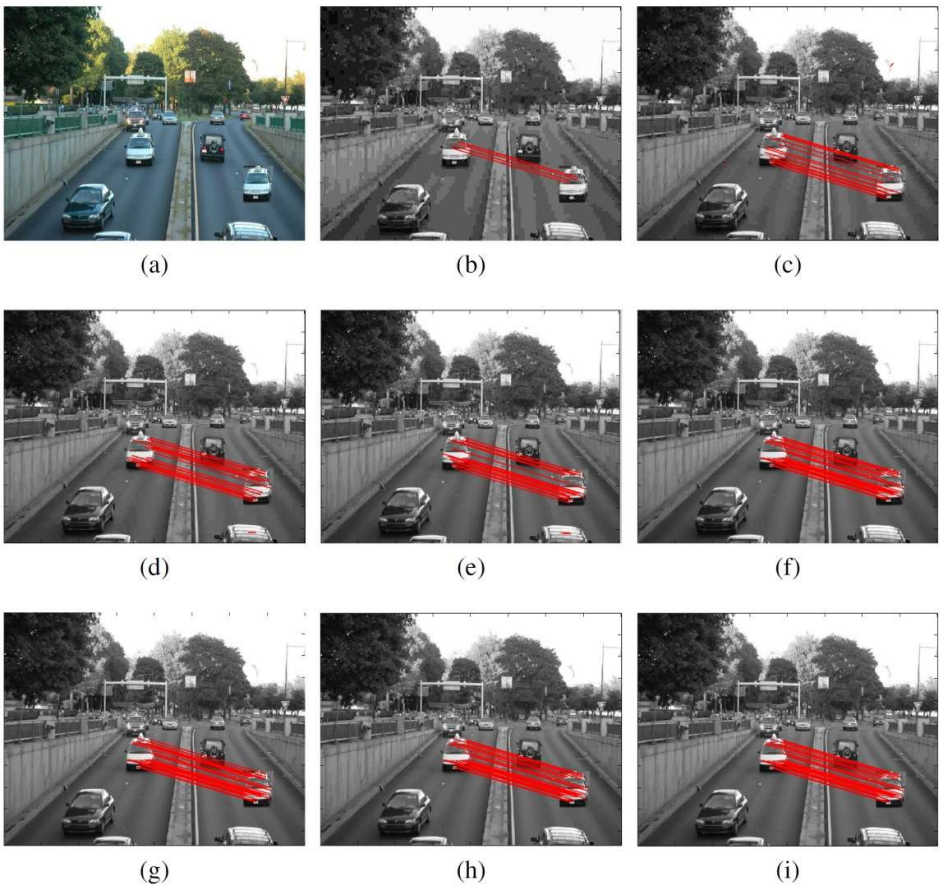

Fig. 7. Regions marked by the proposed method as *tampered* for the same image compressed a various JPEG quality factors.

4.7 Comparison with Conventional Methods

The performance of the proposed method is compared with two other methods using the MICC-F220 dataset. Specifically, the method based on SIFT keypoints [15] and another based on SURF with hierarchical agglomerative clustering [12] are considered as the representative conventional methods. The results in terms of TPR and FPR are recorded in Table 4. It is observed that, when compared with the conventional methods considered, the proposed method achieves 100% TPR as well as the lowest FPR, i.e., 3.12%. Although the method based on SIFT keypoints [14] also achieves 100% TPR, its FPR is rather high, i.e., 8%. The proposed method is better in terms of FPR because clustering keypoints after extraction using centroid clustering method, together with second level of matching contributed in reducing number of false matches.

Table 4. Detection results of the proposed and conventional methods using MICC-F220 dataset.

Methods	FPR%	TPR%
Amerini et al. [15]	8	100
Parul Mishra et al. [12]	3.64	73.64
Proposed Method	**3.12**	**100**

Notably, the proposed method is robust against JPEG compression with different quality factors, which is a significant advantage over the conventional methods. Moreover, the proposed method has a lower FPR than the conventional methods considered. In addition, the proposed method demonstrates high robustness against post-processing operations. Nonetheless, our performance is slightly inferior to the results reported in [23] when the forged areas are small. We shall further improve the performance in detecting and localizing small tampered areas as our future work.

5.0 CONCLUSIONS

In this study, a keypoint-based method (SIFT) was put forward for detecting copy-move forgery in digital image. The proposed method can authenticate digital images and locate duplicated areas generated by copy-move forgery within a reasonable period of time. The proposed technique is also robust against post-processing operations such as JPEG compression, noise or rotation and is capable of detecting multiple forged areas. Experiments were carried out on various datasets comprising of numerous fake and original images. Results prove that the proposed method outperforms other similar methods in terms of FPR and TPR. The false matching rate of the proposed method is effectively reduced, when compared with that of conventional methods. Notably, the FPR is reduced to 3.12%, while the TPR is 100%. Although promising results are attained in detecting copy-move forgeries, we are unable to detect a small forged area because smaller areas have fewer keypoints.

Our future research direction, therefore, is to further enhance the detection performance in handling small tampered area. In addition, different clustering algorithms will be deployed to improve the performance of forgery detection with different clustering, as well as in combination with other detection schemes.

Acknowledgements

This research is supported by Project No.: RG312-14AFR from the University of Malaya.

REFERENCES

[1] Dadkhah, S., et al., *An effective SVD-based image tampering detection and self-recovery using active watermarking.* Signal Processing: Image Communication, 2014. **29**(10): p. 1197-1210.

[2] Lin, Z., et al., *Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis.* Pattern Recognition, 2009. **42**(11): p. 2492-2501.

[3] Ng, T.-T. and S.-F. Chang. *A model for image splicing*. in *Image Processing, 2004. ICIP'04. 2004 International Conference on*. 2004. IEEE.

[4] Li, Y. and H. Wang. *An efficient and robust method for detecting region duplication forgery based on non-parametric local transforms*. in *Image and Signal Processing (CISP), 2012 5th International Congress on*. 2012. IEEE.

[5] Mahdian, B. and S. Saic, *Detection of copy–move forgery using a method based on blur moment invariants.* Forensic science international, 2007. **171**(2): p. 180-189.

[6] Lynch, G., F.Y. Shih, and H.-Y.M. Liao, *An efficient expanding block algorithm for image copy-move forgery detection.* Information Sciences, 2013.

[7] Ryu, S.-J., et al., *Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments.* Information Forensics and Security, IEEE Transactions on, 2013. **8**(8): p. 1355-1370.

[8] Fridrich, A.J., B.D. Soukal, and A.J. Lukáš. *Detection of copy-move forgery in digital images*. in *in Proceedings of Digital Forensic Research Workshop*. 2003. Citeseer.

[9] Dadkhah, S., A.A. Manaf, and S. Sadeghi, *Efficient image authentication and tamper localization algorithm using active watermarking*, in *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*. 2014, Springer. p. 115-148.

[10] Farid, H., *Digital image forensics.* Scientific American, 2008. **298**(6): p. 66-71.

[11] Lowe, D.G., *Distinctive image features from scale-invariant keypoints.* International journal of computer vision, 2004. **60**(2): p. 91-110.

[12] Mishra, P., et al., *Region Duplication Forgery Detection Technique Based on SURF and HAC.* The Scientific World Journal, 2013. **2013**.

[13] Jing, L. and C. Shao, *Image Copy-Move Forgery Detecting Based on Local Invariant Feature.* Journal of Multimedia, 2012. **7**(1): p. 90-97.

[14] Guo, J.-M., Y.-F. Liu, and Z.-J. Wu, *Duplication forgery detection using improved DAISY descriptor.* Expert Systems with Applications, 2012.

[15] Amerini, I., et al., *A sift-based forensic method for copy–move attack detection and transformation recovery.* Information Forensics and Security, IEEE Transactions on, 2011. **6**(3): p. 1099-1110.

[16] Huang, H., W. Guo, and Y. Zhang. *Detection of copy-move forgery in digital images using SIFT algorithm*. in *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*. 2008. IEEE.

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

[18] Kanazawa, Y. and H. Kawakami. *Detection of Planar Regions with Uncalibrated Stereo using Distributions of Feature Points*. in *BMVC*. 2004. Citeseer.

[19] Lindeberg, T., *Scale invariant feature transform.* Scholarpedia, 2012. **7**(5): p. 10491.

[20] Uliyan, D.M., et al., *A novel forged blurred region detection system for image forensic applications.* Expert Systems with Applications, 2016. **64**: p. 1-10.

[21] Sadeghi, S., et al. *Efficient Copy-Move Forgery Detection for Digital Images*. in *Proceedings of World Academy of Science, Engineering and Technology*. 2012. World Academy of Science, Engineering and Technology (WASET).

[22] Muhammad, N., et al. *Copy-move forgery detection using dyadic wavelet transform*. in *Computer Graphics, Imaging and Visualization (CGIV), 2011 Eighth International Conference on*. 2011. IEEE.

[23] Huang, Y., et al., *Improved DCT-based detection of copy-move forgery in images.* Forensic science international, 2011. **206**(1): p. 178-184.

[24] Hou, D.M., Z.Y. Bai, and S.C. Liu, *A New Algorithm for Image Copy-Move Forgery Detection.* Advanced Materials Research, 2012. **433**: p. 5930-5934.

[25] Cao, Y., et al., *A robust detection algorithm for copy-move forgery in digital images.* Forensic science international, 2012. **214**(1): p. 33-43.

[26] M. A. Shayegan, S. Aghabozorgi, R. G. Raj, "A Novel Two-Stage Spectrum-Based Approach for Dimensionality Reduction: A Case Study on the Recognition of Handwritten Numerals," Journal of Applied Mathematics, vol. 2014, Article ID 654787, 14 pages, 2014. doi:10.1155/2014/654787.

[27] Shen, X.J., et al., *Image Copy-Move Forgery Detection Based on SIFT and Gray Level.* Applied Mechanics and Materials, 2013. **263**: p. 3021-3024.

[28] Lin, S.D. and T. Wu. *An integrated technique for splicing and copy-move forgery image detection*. in *Image and Signal Processing (CISP), 2011 4th International Congress on*. 2011. IEEE.

[29] Bo, X., et al. *Image copy-move forgery detection based on SURF*. in *Multimedia Information Networking and Security (MINES), 2010 International Conference on*. 2010. IEEE.

[30] Jalab, H.A. and R.W. Ibrahim, *Texture enhancement based on the Savitzky-Golay fractional differential operator.* Mathematical Problems in Engineering, 2013. **2013**.

[31] Ke, Y. and R. Sukthankar. *PCA-SIFT: A more distinctive representation for local image descriptors*. in *Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on*. 2004. IEEE.

[32] Bay, H., T. Tuytelaars, and L. Van Gool, *Surf: Speeded up robust features*, in *Computer vision–ECCV 2006*. 2006, Springer. p. 404-417.

[33] Li, M. and Y.-m. Cheung, *Automatic lip localization under face illumination with shadow consideration.* Signal Processing, 2009. **89**(12): p. 2425-2434.

[34] Ng, T.-T., et al., *Columbia photographic images and photorealistic computer graphics dataset.* Columbia University, ADVENT Technical Report, 2005: p. 205-2004.