A Forensic Scheme for Revealing Post-processed Region Duplication Forgery in Suspected Images

Diaa Mohammed Uliyan[1], Mohammed A. Fadhil Al-Husainy[1], Ahmad Mousa Altamimi[2], Hamid Abdullah Jalab[3]

[1]*Faculty of Information Technology, Department of Computer Science, Middle East University, Amman, Jordan*

[2]*Faculty of Information Technology, Department of Computer Science, Applied Science Private University, Amman, Jordan*

[3]*Faculty of Computer Science & Information Technology, University of Malaya, Kuala Lumpur, Malaysia*

duliyan@meu.edu.jo

***Abstract*—Recent researches have demonstrated that local interest points alone can be employed to detect region duplication forgery in image forensics. Authentic images may be abused by copy-move tool in Adobe Photoshop to fully contained duplicated regions such as objects with high primitives such as corners and edges. Corners and edges represent the internal structure of an object in the image which makes them have a discriminating property under geometric transformations such as scale and rotation operation. They can be localised using scale-invariant features transform (SIFT) algorithm. In this paper, we provide an image forgery detection technique by using local interest points. Local interest points can be exposed by extracting adaptive non-maximal suppression (ANMS) keypoints from dividing blocks in the segmented image to detect such corners of objects. We also demonstrate that ANMS keypoints can be effectively utilised to detect blurred and scaled forged regions. The ANMS features of the image are shown to exhibit the internal structure of copy moved region. We provide a new texture descriptor called local phase quantisation (LPQ) that is robust to image blurring and also to eliminate the false positives of duplicated regions. Experimental results show that our scheme has the ability to reveal region duplication forgeries under scaling, rotation and blur manipulation of JPEG images on MICC-F220 and CASIA v2 image datasets.**

***Index Terms*— Copy-Move Forgery; Image Forgery Detection; Image Forensics; Local Interest Points; Region Duplication; Segmented Regions.**

I. INTRODUCTION

In the digital era, it is quite popular for expert users of image editing tools to manipulate images easily. Nowadays, we are facing the abuse of digital image tools; image forgery has begun to crumble the trustworthiness of visual images [1], that seeing is no longer believing. Image forgery has inspired researchers [2] to investigate and check the authenticity of digital images due to its effect to the judgment of the truth of suspected images in many sectors, such as digital newspapers, law evidence and medical documents. Region duplication forgery is one of the most common image editing tools to abuse image. It is a simple operation that gives a high visual impact to suspected images. Furthermore, it is known as copy-move, cloning or region duplication. Copy-move forgery duplicates a region of an image and moves it to another location within the same image. This type of forgery has a good effect which conveys misleading information in order to support an individual agenda.

Some existing methods are developed to examine and locate copy-moved regions in a forged image [3, 4]. Some can detect duplicate regions [5-7] and another can locate multiple duplicated regions [8]. The region duplication forgery detection methods have been categorised and evaluated based on their sensitivity towards two types of attacks: a) Geometrical manipulation attacks and b) Postprocessing attacks. For a geometrical attack, the copy-move detection methods are resilient against spatial domain changes such as rotation [9], scaling [10, 11]. Conversely, some scientific papers have examined the robustness against the retouching or blending tools which hide visual editing artefacts in the image through some post-processing attacks. Such attacks include: blurring [12, 13], additive noise [14] and JPEG compression [15, 16] impacts are obtained after applying geometrical transformation operations. Hence, this type of forgery is a challenging problem that motivates us to investigate forged images against scale, rotation and blur attacks. As blurring could transform the features of any region in the image, further inspection of this attack should consider [12]. The blur transformation in the image features may also make the standard copy-move forgery detection methods struggle to detect the blurred duplicated regions. The proposed method starts a forensic job by collecting images that contain simple transformation attacks and blur attacks. The original images are collected from the Dataset MICC-F220 [17] and CASIA v2.0 [18]. Then, the proposed method is implemented to combine the scale invariant feature with LPQ matching technique. We compare the performance of the proposed method by F-scores with state-of-the-art methods: keypoint based methods [17, 19, 20] and block-based methods: [21, 22].

The paper is organized into five sections. Section II highlights Related Works on copy-move forgery detection per some attacks included. Section III introduces the proposed method. In section IV, it will discuss the experimental results and performance evaluation. In section V, the conclusion and future works are summarised.

II. RELATED WORKS

The common flowchart of most copy-move forgery detection methods has six steps as shown in Figure 1. These steps are: 1) image preprocessing, 2) image division, 3) feature extraction, 4) building descriptor 5) matching and 6) show detection results.

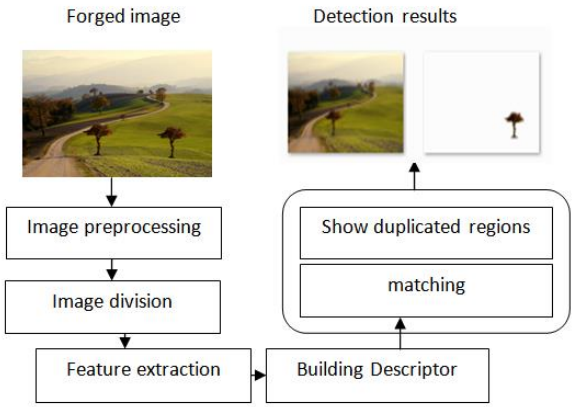


Figure 1: The basic flowchat of standard copy-move forgery detection sechemes [14].

The first step is optional, which tries to improve the image content by defeating undesired noise. The most frequent preprocessing step is image colour conversion be converting an RGB colour image into a grayscale image [23] by using Equation (1).

$$Grayscale = 0.228\,R + 0.587\,G + 0.114\,B \qquad (1)$$

where R,G and B channels represent the Red, Green and Blue channels as pixel information in the image.

Rafsanjany et al. [24] convert the input RGB image to Grayscale and Lab colour space. Then, they divided it into square blocks to extract features. Their method achieved about 90% F-measure for JPEG images with size 512x512. Another colour conversion is used such as YC_bC_r colour system to give the luminance information Y or chrominance information C_b and C_r [25]. Shinfeng et al. [26] used the YC_bC_r colour system for image conversion and divided it into blocks, for each block, DCT coefficients are extracted to produce 64-bit feature vector. Later, they computed the probability of each block by identifying the period of its histogram.

The main goal of the image conversion is to achieve the dimensionality reduction of the image features and extract the distinctive local interest points or visual features. This could help with performance the proposed copy-move forgery detection methods in the aspect of time complexity [27]. Similarly, Hue saturation value (HSV) colour space is used in method [28], which help to detect intense dark duplicated regions or bright regions with around 7.22 % false positive rate.

Based on the way of dividing the image on the second stage of copy-move forgery detection, these techniques are classified into three classes: block-based schemes [29], segmented regions-based schemes [6] and local keypoints based schemes [14]. In the block-based, the image is divided into a number of sub-blocks either square blocking or circle blocking. Similarly, the segmented-based method tries to segment the image into different regions that fully covered the forged objects in the image based on colour, texture and property palette properties. Conversely, the keypoint based method detects local interest points to find primitive features in the image. The benefit of this stage is that can minimise the time complexity for matching steps in order to search the similar feature vectors of building descriptor in an image compared to exhaustive search.

After image division, the feature extraction can help to choose the relevant data that exhibit the internal structure and its properties in the image. These features are saved into a feature vector. Finally, matching between two feature vectors is employed using the distance of the nearest neighbour from all points in the feature space to show forged regions.

Based on copy-move forgery detection steps, common schemes focused on image division and feature extraction steps that exhibit invariant features against geometric transformation and post-processing attacks. These schemes are introduced in detail [30] as follows:

1) Block-based methods

These methods divide the image into square or circle blocks to extract features from these blocks as shown in Figure 2. The main advantage of this approach is that give high detection accuracy for the textured forged regions. However, it still gives high computational complexity due to the exhaustive search between divided blocks in the image [29].

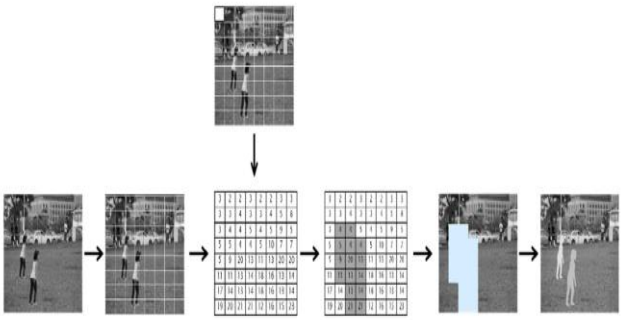


Figure 2: The image is divided into 8x8 blocks, features are highlighted and saved for the matching process.

2) Segmented-based methods

These methods segment the input image into homogeneous regions based on colour or texture. This approach works well in the forged images that have duplicated objects [31].

3) Keypoint-based methods

These methods discard block division step and use local interest point detectors to extract features. These features are distinctive to represent corners, edges or blobs in the image. Then, a robust texture descriptor is built to increase reliability against geometric transformation attacks [32].

Different types of attacks have been considered in existing methods for detecting region duplication forgery [33]. These methods are called Passive methods due to detecting image forgery without requiring explicit prior information. The main goal is to analyse the history of the image tampering blindly by examining pixel-level correlations [34].

In this article, popular feature extraction methods in copy-move forgery detection methods were covered for various geometric transformations and postprocessing attacks. The robustness of detection methods depends on invariant features to possible attacks as pointed in [3]. Copy-move forgery detection methods based on the type of features are classified into two classes: Frequency transform methods [35], Texture and intensity-based methods [16].

1) Frequency transform methods

These methods convert the image pixel information into the frequency domain to extract high-frequency coefficients to

form the image. This approach is robust to JPEG compression and can detect duplicated regions with a large size 128 x 128 pixel. The limitations are the high computational complexity and struggle to detect duplicated regions with scale and rotation attacks. The frequency features are: discrete cosine transform (DCT) [8], Fourier transform (FT) [32], discrete wavelet transform (DWT) [5], curvelet transform (CT)[36] and Wiener filter. The limitation of this approach is that features are sensitive to blur attack.

2) Texture and intensity-based methods

These methods extract features that exhibit image texture regions with the smoothness property. Various features have been used to detect textured duplicated regions in copy-move forgery detection methods. For instance, local binary patterns (LBP), histogram of gradient (HOG), Zernike moments (Zm) [37] which is robust to rotation, log-polar transform [38] that detects rotated duplicated regions, principal component analysis (PCA) and singular value decomposition (SVD) that reduce the size of feature vector to enhance the time complexity.

All of these methods that utilise frequency and texture features were employed in block-based methods and did not suppose that forged regions may be geometrically transformed. Another direction has been discovered to detect duplicated regions against scaling and rotations.

This can be done by the keypoint-based approach, for instance, Scale-invariant transform features (SIFT), speed up robust features (SURF) [39] and Harris features. These features are slightly blurred invariant. This motivates us to develop a blur invariant detection method to detect blurred forged duplicated regions in the suspected images.

Blurring is made effectively through image forgery process suing averaging of neighbour pixels in a square block [40]. The blur is commonly applied by Gaussian, defocus and motion blurs. In practice, the Gaussian blur filter is well known by users that do tampering in the image due to its simplicity. If the duplicated region is retouched by blur, then the main features of the blurred region are minimised and details cannot be seen.

Blurring on forged regions aims to manipulate the region's information and assists in hiding retouch and blending artefacts. As a result, blurring allows the duplicated region to be consistent with its surrounding area. The scope of locating tampered regions attacked by blurring artefact is even smaller. Only a few related papers have been discovered that deal with blur attack [13, 40-44].

The first attempt was made by [43] to detect blurred duplicated region forgery. The extracted blur invariant moments from image blocks. Then, Principal Component Analysis was employed to achieve the dimensionality reduction of feature vectors. Finally, they used a kd tree to locate the duplicated regions. The weakness of their method is that struggle to detect uniform duplicated regions and also gives high false positives. Another blur detection method is developed by Zhou et al. [40] for revealing blurred edges in the duplicated regions. Their method starts by preprocessing step to convert the image into binary one. Then, the method applied edge-preserving–smoothing filters, followed by a mathematical morphology operation using the erosion filter to expose forged duplicated area with malicious blurred edges. The average accuracy rate of about 89.26% in images with blurred edges manually attacked by the Gaussian noise filter. Zheng et al. [45] located tampered regions with blur attack via wavelet homomorphic filtering to represent pretty high-frequency edges. Then, erosion operation was applied to expose blurred edges in the forged region from normal regions which effectively reduced the false positive rates. Wang et al. [41] used non-subsampled contourlet transform (NCST) to examine manually blurred edges from duplicating regions. The detection of forged duplicated regions is done using a support vector machine (SVM). In [13], blur artefacts were explored in forged regions by using combined blur and affine transform moments. The relative detection error was employed to estimate the stability of local invariant features deformed by Gaussian and motions blurs. The method achieved a high accuracy rate with the small feature vector. Guzin et al. [46] applied Object Removal operation from Uniform Background Forgery by adapting accelerated diffusion filter (AKAZE). The Local binary difference descriptor was built in AKAZE features which are scale invariant features. The size of the feature vector is 486 bits. The performance of their method in terms of TPR is 85.74%, 71.35% and 76.73% against Gaussian blurring, rotation and JPG compression respectively.

The paper proposed a region duplication forgery detection scheme based on ANMS features and LPQ texture descriptor. In this paper, a part of the authentic image is copied and pasted to another area to mislead the semantic visual meaning of the image. While the copy-move operation is applied, the duplicated region may be post-processed using rotation, scaling, blurring to create a better forgery. The common pipeline of the proposed method is, first the input image is segmented-based on colour features. The fuzzy C-means method is used to cluster and label the segments in the image. The centroid of each segment is located in the image. We assume that forgery is made by for small regions. These regions can be detected by calculating the least frequent occurrence of labeled segments in the image. For each candidate segment, ANMS local interest points are extracted. ANMS features are scale invariant to represent the structure of the segmented region. Second, each segment is split into four blocks; the size of the block is 4 x 4. The distribution of ANMS points the blocks of each segment contributes to detect duplicated regions against rotation. Third, blur invariant LPQ descriptor is built to the approximation of the ANMS points in each segment. Finally, the closest local keypoint search of features between two segments is employed by a generalised nearest neighbour (G2NN) to improve the performance of our method in terms of true positive rate (TPR) and false positive rate (FPR).

III. PROPOSED METHOD

In this section, we introduce in detail the flowchart of the proposed method for exposing the copy-move forgery, with scaling and blurring of the cloned region. Our contribution is proposing a forensic keypoint-based method for blur and scale invariant copy-move forgery detection in digital images. A diagram representing the workflow of the proposed technique is shown in Figure 3.

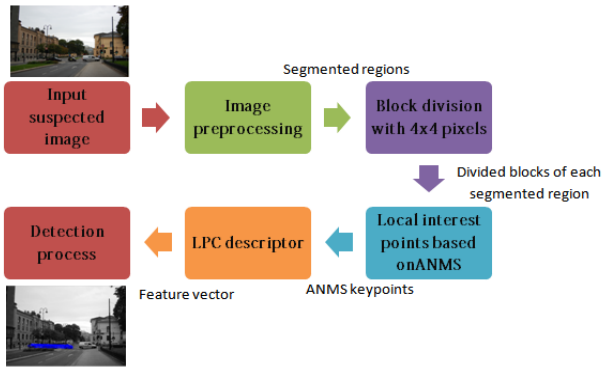


Figure 3: The flowchart of the proposed forensic detection scheme to show the copy moved region match with original one highlighted by the blue matching line between ANMS keypoints.

A. *Image Preprocessing with Colour Segmentation*

Image segmentation is one of the most important techniques for image analysis and object detection [47]. The main aim of Segmentation of our method is to perform an efficient search strategy to detect duplicated regions such objects in the image. It starts from coarse search to quickly split an image into homogeneous objects based on discontinuity and similarity of image intensity values. Then a feature extraction is applied to these query regions to improve the TPR of copy-move forgery detection. The proposed colour segmentation approach, followed by fuzzy c-means clustering (FCM) is introduced in [48]. The fuzzy c-means is an unsupervised technique which estimates the RGB channel of every pixel in the image and compares it with the centroid of the cluster. It makes a decision about which category the pixel should relate to. Each pixel in the image should be in [0-1], which the value describes how much pixel value relates to its cluster. A fuzzy membership criterion denotes that the sum of the membership value of a pixel to all clusters equals 1. The FCM clustering is an iterative optimisation that minimises the cost function which is described as follows:

$$J = \sum_{i=1}^{n} \sum_{k=1}^{c} \mu_{ik}^{m} |p_i - v_k|^2 \quad (2)$$

where, an image I with n pixels to be partitioned into c clusters, p_i represents the i^{th} image pixels. μ_i is the fuzzy membership value with fuzziness factor k >1. Here, the membership function μ_i with the centroid of K^{th} cluster V_k is defined as follows:

$$\mu_{ik} = \frac{1}{\sum_{l=1}^{c} \left(\frac{|p_i - v_k|}{|p_i - v_l|} \right)^{2/m-1}} \quad (3)$$

$$v_k = \frac{\sum_{i=1}^{n} \mu_{ik}^{m} p_i}{\sum_{i=1}^{n} \mu_{ik}^{m}} \quad (4)$$

Here, v_k denotes to the centroid of the k^{th} cluster and $|p_i - v_k|$ refers to the Euclidean distance between two points: p_i and v_k. By using the cluster information (c=5, the maximum number of iterations=10) and the pixel information pi from the forged image, I with size 512 x 512, the homogeneous regions including copy-moved regions can be extracted as shown in Figure 4.

(a) (b) (c)

Figure 4: (a) Original image, (b) suspected image with duplicated regions and (c) Segmented image using the FCM algorithm.

B. *Adaptive Non Maxima Suppression (ANMS) Features*

Keypoint-based methods are significantly helpful in detecting visual objects in the image. While the block-based schemes split the image into blocks, keypoint-based schemes identify and highlight only regions with high entropy, called the local interest points or keypoints. However, key points such as SIFT are robust against geometric transformations such as scaling. However, the major drawback is that keypoints may be insufficient or even none in the forged region of uniform texture. To avoid the drawback of SIFT-based methods, we adopt the ANMS method which is an effective approach suggested by Brown, Szeliski, & Winder [49] to select uniformly distributed interest points for instance, $K = \{K1, K2, \ldots, K_m | K \in (\mu_{K_m}, V_{K_m})\}$ in image and provide the stability and good performance in scale and rotation through detection of duplicated regions. The principal of ANMS is to select $K_m \in K$, K_m is the maximum neighborhood of region of interest with radius r pixels. K are generated from Harris corners have can be described in Equation (5).

$$E(\mu, v)|_{(x,y)} = \sum w(x,y)[I(x+u, y+v) - I(x,y)]^2 \quad (5)$$

where w(x,y) denotes a Gaussian kernel defined below and (u,v) is the minimal Euclidean distance.

$$w(x,y) = \exp\left(-\frac{1}{2}(u^2 + v^2) \Big/ \sigma^2\right) \quad (6)$$

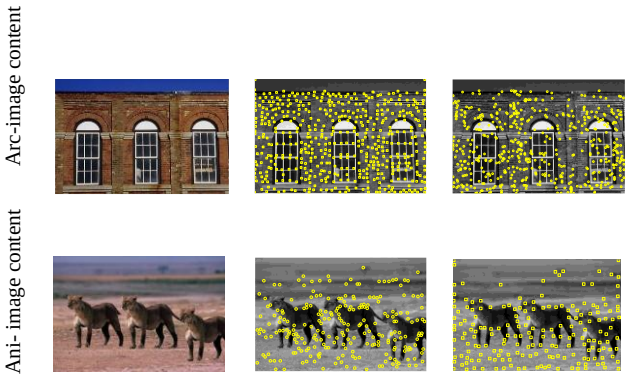
where σ is the Standard Deviation. Then, Taylor series expansion is employed to the equation of $E(\mu, v)$ to eliminate the weak interest points as follows.

$$A = w.I_{x^2}, B = w.I_{y^2}, C = w.I_x \quad (7)$$

Here, denotes the image convolution operator. I_x, I_y are the horizontal and vertical directions in the image *I*. a corner response measure is defined as follows.

$$Z = \det(V) - \alpha \times tr^2(V), \text{ where } V = \begin{bmatrix} A & C \\ C & B \end{bmatrix} \quad (8)$$

in which, V is a matrix has two eigenvalues. tr is the race of a matrix and $\alpha = 0.06$ in our method. Figure 5 shows the results obtained by the ANMS compared with the SIFT based method [50]. ANMS points are much better distributed in the image and represent the structure of windows object by local interest points such as corners. In Figure 5, two types of images are regarded: (a) Arc - architecture content and (b) Ani - animal content.



(a) Forged image (b) ANMS features (c) SIFT features

Figure 5: Keypoints detected from Forged images in column (A) by B) ANMS method and C) SIFT method.

C. *Local Phase Quantization (LPQ) descriptor*

Ojansivu et al. [51] proposed a blur invariant method to extract phase information in the Fourier transform domain and consider only the best energy of sampling low frequencies varying with blur changes. The blurring process in LPQ is applied by convolving the image with a Point Spread Function (PSF) as follows.

$$g(x,y) = (f * h)(x,y) + n(x,y) \quad (9)$$

where, where g(x, y) denotes a blurred image, f(x, y) represents the original image. h(x, y) is the PSF of blur and n(x, y) is the additive noise. Here * is the image convolution operator. When the image is blurred with PSF, then we extract the Fourier transform features regarding the frequency domain by Equation (10).

$$G(u,v) = (F * H)(u,v) + N(u,v) \quad (10)$$

where G(u,v) denotes to the discrete Fourier transforms (DFT) of the blurred PSF image g(x,y). Here, F(u,v)=DFT(f(x,y)), H(u,v) is the blur PSF kernel for the F(u,v). As a result, the image G(u,v) has frequency coefficients in the blurred image. After applying the Fourier transform, the image will have two parts: the real part $Re(u,v)$ and imaginary part $Im(u,v)$. Only real valued will be kept as follows.

$$G(u,v) = |Re\{F(u,v)\}| + |Im\{F(u,v)\} \quad (11)$$

Real value parts are quantised based on scalar quantizer as follows.

$$q_i = \begin{Bmatrix} 1, & if\ Re_i(u,v) \geq 0 \\ 0, & otherwise \end{Bmatrix} \quad (12)$$

Here $q_i$is the i[th] component of $Re(u,v)$. The quantized coefficients are integer values between 0-255.

Finally, the LPQ descriptor, which is similar to the local binary pattern (LBP) [16] and is calculated as follows.

$$LPQ(x,y) = \sum_{j=1}^{j=8} q_i(x,y)^{\,2^{\,j-1}} \quad (13)$$

In Figure 6, an example of the computing LPQ for sample images from the CASIA dataset and the duplicated regions are recognised.

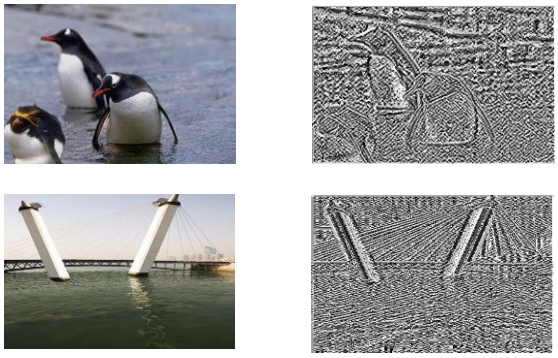


Figure 6: LPQ descriptor of sample images on CASIA v2.

D. *Forgery localisation process*

As discussed previously, keypoints for each segmented region are extracted by ANMS. The LPC descriptor for each segment in the image was calculated to do matching between keypoints and discover the duplicated regions. The best matching between keypoints is founded by a generalised nearest neighbour (G2NN) [17]. In G2NN, a ratio between closest keypoint $d_i$with the second nearest neighbor d_{i+1} is calculated as follows:

$$d = \frac{d_i}{d_{i+1}} \leq T, \quad T \in [0,1] \quad (14)$$

where d is Euclidean Distance, T is threshold value=0.89 in our experiments. x denotes the value on which the iterative procedure G2NN stops, then every keypoint related to a calculated distance in $\{d1, d2, d3, d4 \ldots\ldots dx\}$ satisfies $1 \leq x < n$, is regarded to be matched for keypoint. However, to search the similarity between two local keypoints, simply the proposed method evaluates the distance between two descriptors with respect to a global threshold *T*.

IV. Experimental Results

The performance of the blur invariant detection method was examined through a set of forged images. These images were collected from two standard datasets, namely MICC-F220 and CASIA v2. Firstly, we introduce the experimental setup of our method and performance evaluation metric where used for detecting duplicated regions. These regions have repetitive texture patterns which are required to make a convinced forgery via post-processing operation such as blurring and scaling. Then, the proposed method is evaluated with existing methods developed in [17], [31] and [20]. The details of the experiments are discussed.

A. *Evaluation Metric*

Our method is developed by MATLAB R2014a on Intel Core i5 processor, with 16 GB memory. The forged images under copy-move forgery were collected from the first Dataset MICC-F220 which are produced by a well-known copy-move forgery detection method [17]. It consists of digital images from the Columbia photographic image repository [52] and their personal collection. MICC-F220 includes of 220 images with various sizes from 722 x 480 to 800 x 600 pixels. The size of the duplicated regions conceals about 1.2% of the whole image. The second Dataset (CASIA v2) has about 5123 forged images in JPEG Format with various quality factors. The image resolutions are varying

from 240×160 to 900×600. A duplicated region on these images was copied and moved with considering the post-processing after copy move operation to finish the fake image generation; simple postprocessing attacks comprising scaling, rotation, blurring, JPEG compression and additive noise.

Here, A Gaussian blur filter is applied in duplicated pattern regions. The similarity threshold is set experimentally to T = 0.8 which give a high detection rate. The performance of the proposed detection scheme is evaluated via the True Positive Rate (T_{PR}) and False Positive Rate (F_{PR}). The evaluation metric is defined to include others: True positive (TP), True negatives (TN), False positives (FP), False negatives (FN) and F-score calculated in [6, 46] as follows:

$$F_{score} = \frac{2Tp}{2Tp+FN+FP} \quad (15)$$

$$T_{PR} = \frac{\text{No.of detected images as forged being forged}}{\text{No.of forged images}} \quad (16)$$

$$F_{PR} = \frac{\text{No.of detected images as forged being original}}{\text{No.of original images}} \quad (17)$$

where TP is the number of exposed forged images, FN is undetected forged images, and FP is incorrectly detected original images.

B. Region Duplication Forgery Without Attacks

Normal forgery is defined as creating a forged image without applying any attacks to the original part or on the whole image. In Figure 7, the small car has been copied and pasted to another area of the image without applying any attack on the original part, as results illustrate our method has better detection results compared with SIFT-based method [17]. This is due to a number of local keypoints detected by the ANMS directly improving the detection rate in the image. Here, the number of keypoints detect by our method in the Car image is 70 while another method detects 50 keypoints only. More key points are selected means better performance regarding T_{PR}. However, it will spend much time than Sift based method. The average detection time of the proposed method is about 13.8 seconds.

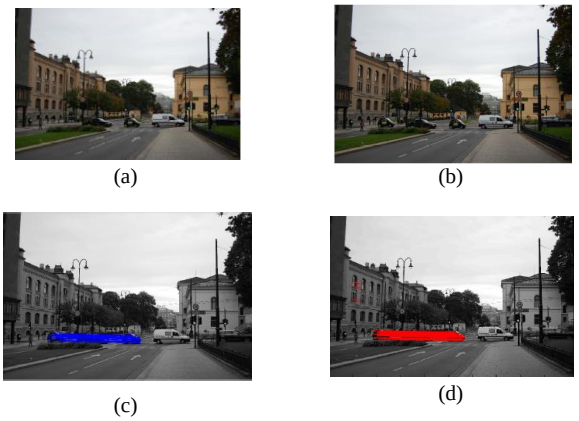


Figure 7: (a) Original image, (b) Forged image with Normal forgery, (c) Detection result of our method with T_{PR}=0.96, (d) Detection result of SFIT based method with T_{PR}=0.94 and F_{PR}=0.07.

1) Scale attacks

To examine the proposed method under scaling attack, Various scaling transformations with scaling Factors (SF=0.5,0.7,1,1.5) have been applied to images (A-D) in the dataset: MICC-F220, where Sx and Sy are scale factors applied to the x and y-axis of the image part as shown in Figure 8.

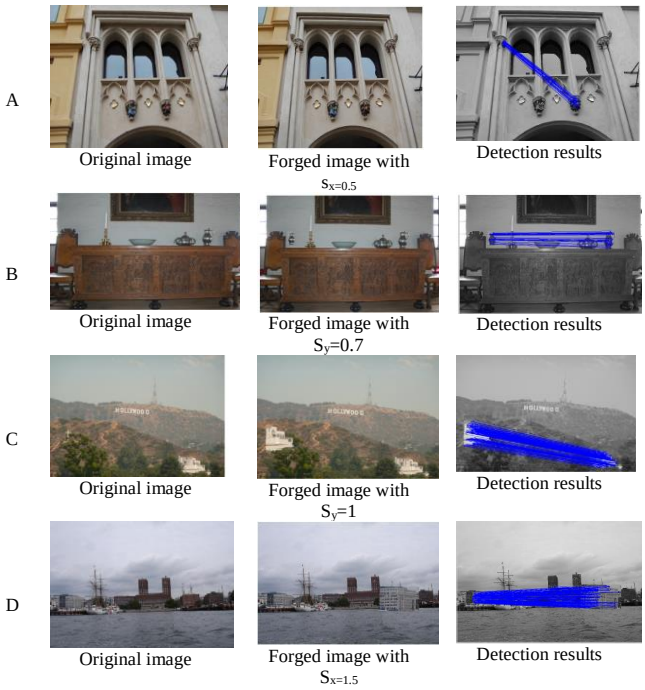


Figure 8: Detection of duplicated regions with horizontal and vertical scaling attacks.

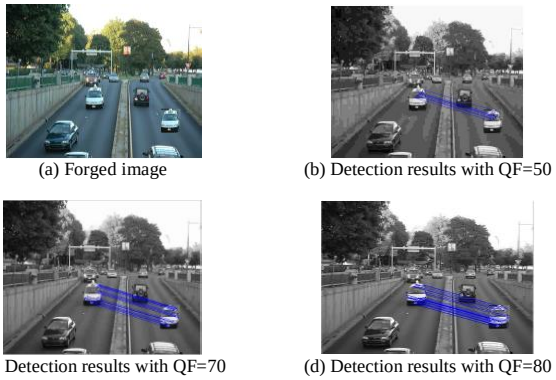
Furthermore, the proposed method is examined to identify the optimal threshold T in the detection step to achieve the best detection rate for scaling attack. Table 1 shows that the value of 0.8 is identified as the best threshold value where the best true positive rate (TPR) and false positive rate (FPR) results are achieved. The goal of our method is achieved the lowest FPR which means only a few percents of all images did not authenticate correctly; the TPR value is about 0.96 which means the majority of images in a dataset are authenticated correctly.

Table 1
Threshold Estimation for Images in MICC-F220 Under Scale Attack with Scaling Factors (SF=0.5, 0.7, 1, 1.5).

Threshold Value	Average T_{PR}	Average F_{PR}
0.1	0.75	0.20
0.3	0.80	0.36
0.5	0.90	0.10
0.7	0.92	0.12
0.8	**0.96**	**0.07**

2) JPEG compression

Some experiments for JPEG compressions are addressed. The performance of our method is evaluated on a set of images compressed with various quality factors (QF=80, 70 and 50) as shown in Figure 9. The ROC curve in Figure 10 shows that the TPR and FPR of the proposed method are 90%, 4% respectively for JPEG quality factors up to 40.



(a) Forged image (b) Detection results with QF=50

(c) Detection results with QF=70 (d) Detection results with QF=80

Figure 9: The ability of our method to detect duplicated regions via various JPEG factors.

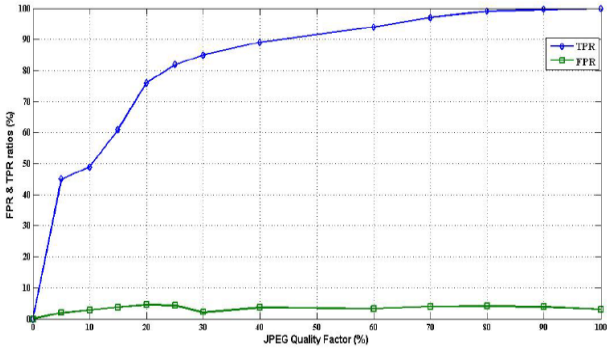


Figure 10: ROC curve in terms of TPR and FPR based on MICC-F220.

As shown in Figure 10, it can be concluded that the proposed method is still reliable and robust against JPEG compression even with a low-quality factor such as Q=50.

3) Forgery with different block sizes

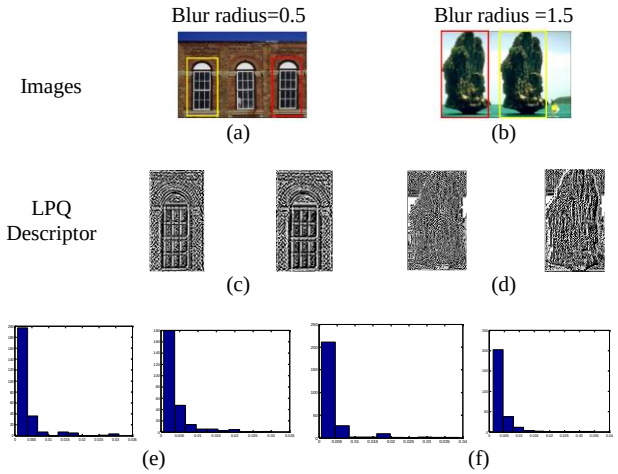
100 original images from CASIA v2 image are selected. For each original image and each duplicate region with a block size 32x32 pixels, 64x 64pixels and 96 x96 pixels, four forged images are created with the additive noise duplicated regions by SNRs (dB=10, 15,20,30). This results in 400 forged images in total. The detection performances of duplicated regions for each block size with additive noise are presented in Table 2. It shows the efficiency of the system in case of very high signal-to-noise ratios.

Table 2
The Detection Performance of Region Duplication Forgery with Different Block Size from Images in CASIA v2

SNR (dB)	Block size 32 x 32		64 x 64		96 x 96	
	T_{PR}	F_{PR}	T_{PR}	F_{PR}	T_{PR}	F_{PR}
10	0.96	0.06	0.95	0.06	0.97	0.03
15	0.96	0.08	0.94	0.08	0.96	0.08
20	0.95	0.08	0.93	0.08	0.95	0.15
30	0.94	0.10	0.93	0.10	0.95	0.15

4) Blur Invariant Features

Some experiments of detecting region duplication forgery under blur with their corresponding descriptors constructed by our method. Here, we use Gaussian blurs with a radius varying from 0.5 to 2. The details are shown in Figure 11.



Histograms of selected regions in LPQ descriptor

Figure 11: Illustrating region duplication forgery detection by local phase quantised coefficients from images on CASIA v2. (a) Image "window" has blurred duplicated region with (Gaussian blur radius = 0.5) which highlighted by the red rectangle. Image (b) has blurred duplicated region with (Gaussian blur radius = 1.5). (c) and (d) are LPQ image maps of (a) and (b) to extract significant features of the internal structure of foreground objects. (e) and (f) The histograms of selected regions in LPQ descriptor show the similarity of features between the blurred region and Normal region.

C. Comparative Study

As shown in Table 3, the proposed method is examined with well-known state-of-the-art methods such as keypoint-based methods: [17], [19], [20] and block-based methods: [21], [22]. These methods focused on detecting region duplication forgery with different post-processing attacks, for instance, scaling and blurring.

Table 3
The Overall Performance of the Proposed Compared with The State-Of-The-Art Methods on MICC-F220.

Methods	T_{PR}	F_{PR}	F_{score}	Features	Block size	Time (s)
[17]	100	8	81.40	SIFT	NA	4.94
[19]	73.6	3.64	N/A	SURF and HAC	4 x4	2.58
[20]	94.08	1.70	N/A	SURF on HSV color features	Circle block with radii=4	18.81
[21]	96.579	NA	75.166	DCT	4 x4	296.74
[22]	96.606	NA	96.05	stationary wavelet transform (SWT)	4 x4	NA
The proposed method	97	3	97.05	ANMS and LPQ	4 x 4	13.80

Table 3 shows that the proposed scheme gives a TPR=97% which is better than TPRs in the methods: [19] and [20] due to the robustness of ANMS features against scale and blur attacks compared with SURF features. [17] method gives high FPR due to the weakness of SIFT method to detect local keypoints of duplicated regions when the textures of some forged regions are almost in uniform, since the local extrema may not exist in such region. The FPR is about 3% which is less than FPR of [19] method due to G2NN clustering technique to find the best matching.

The proposed method extracts local phase quantised

coefficients from divided regions 4x4 in the image. LPQ texture descriptor is insensitive to blurring manipulations which gives a high F-score=97% for detecting this type of forgery compared with [21] method and [22] method.

V. Conclusion

In this paper, robust features such as local interest points play an important rule to expose copy-move forgery on images. ANMS keypoints and LPQ texture descriptor have been proposed. The use of image preprocessing like colour segmentation has reduced the FPR in the suspected image. Clustering segmented regions in the image based on fuzzy C means will increase the TPR of matching duplicated regions over ANMS keypoints. From the suspected forged images, the proposed method can find the duplicated regions, even if they are post-processed by some transformations like scaling or blurring. Future works will focus on image forgery with reflections and illumination changes.

Acknowledgement

The authors are grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

References

[1] H. Farid, "Digital image forensics," *Scientific American*, vol. 298, pp. 66-71, 2008.
[2] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," *Forensic science international*, vol. 224, pp. 59-67, 2012.
[3] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1841-1851, 2012.
[4] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," *Forensic science international*, vol. 231, pp. 284-295, 2013.
[5] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digital Investigation*, vol. 9, pp. 49-57, 2012.
[6] D. M. Uliyan, H. A. Jalab, A. Abuarqoub, and M. Abuhashim, "Segmented-Based Region Duplication Forgery Detection Using MOD Keypoints and Texture Descriptor," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017, p. 3.
[7] D. M. H. Uliyan, "Region Duplication Forgery Detection Technique Based on Keypoint Matching," Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya, 2016.
[8] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic science international*, vol. 233, pp. 158-166, 2013.
[9] D. M. Uliyan, H. A. Jalab, A. W. Abdul Wahab, and S. Sadeghi, "Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points," *Symmetry*, vol. 8, p. 62, 2016.
[10] J.-M. Guo, Y.-F. Liu, and Z.-J. Wu, "Duplication forgery detection using improved DAISY descriptor," *Expert Systems with Applications*, vol. 40, pp. 707-714, 2013.
[11] D. M. Uliyan and M. A. Al-Husainy, "Detection of Scaled Region Duplication Image Forgery using Color based Segmentation with LSB Signature," *International Journal Of Advanced Computer Science And Applications*, vol. 8, pp. 126-132, 2017.
[12] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, P. Shivakumara, and S. Sadeghi, "A novel forged blurred region detection system for image forensic applications," *Expert Systems with Applications*, vol. 64, pp. 1-10, 2016.
[13] T. Wang, J. Tang, and B. Luo, "Blind detection of region duplication forgery by merging blur and affine moment invariants," in *Image and Graphics (ICIG), 2013 Seventh International Conference on*, Qingdao, China, 2013, pp. 258-264.
[14] S. Sadeghi, H. A. Jalab, K. Wong, D. Uliyan, and S. Dadkhah, "Keypoint based authentication and localization of copy-move forgery in digital image," *Malaysian Journal of Computer Science*, vol. 30, pp. 117-133, 2017.
[15] X.-h. Li, Y.-q. Zhao, M. Liao, F. Shih, and Y. Shi, "Passive detection of copy-paste forgery between JPEG images," *Journal of Central South University*, vol. 19, pp. 2839-2851, 2012.
[16] D. M. Uliyan, H. A. Jalab, and A. W. A. Wahab, "Copy move image forgery detection using Hessian and center symmetric local binary pattern," in *Open Systems (ICOS), 2015 IEEE Confernece on*, 2015, pp. 7-11.
[17] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," *Information Forensics and Security, IEEE Transactions on*, vol. 6, pp. 1099-1110, 2011.
[18] H. Z. Peng Gao, Ruier Guo, Jingli Liu, Lihu Ma, Jin Zhang and Qian He. (2009, 23, May 2016). *CASIA Image Tempering Detection Evaluation Database (CAISA TIDE) V2.0*. Available: http://forensics.idealtest.org/casiav2/
[19] P. Mishra, N. Mishra, S. Sharma, and R. Patel, "Region duplication forgery detection technique based on SURF and HAC," *The Scientific World Journal*, vol. 2013, 2013.
[20] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," *Journal of Visual Communication and Image Representation*, vol. 29, pp. 16-32, 2015.
[21] M. H. Alkawaz, G. Sulong, T. Saba, and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Computing and Applications*, pp. 1-10, 2016.
[22] T. Mahmood, Z. Mehmood, M. Shah, and Z. Khan, "An efficient forensic technique for exposing region duplication forgery in digital images," *Applied Intelligence*, pp. 1-11, 2017.
[23] F. Peng, Y.-y. Nie, and M. Long, "A complete passive blind image copy-move forensics scheme based on compound statistics features," *Forensic science international*, vol. 212, pp. e21-e25, 2011.
[24] R. Kushol, M. S. Salekin, M. H. Kabir, and A. A. Khan, "Copy-Move Forgery Detection Using Color Space and Moment Invariants-Based Features," in *Digital Image Computing: Techniques and Applications (DICTA), 2016 International Conference on*, 2016, pp. 1-6.
[25] G. Muhammad, M. H. Al-Hammadi, M. Hussain, A. M. Mirza, and G. Bebis, "Copy move image forgery detection method using steerable pyramid transform and texture descriptor," in *EUROCON, 2013*, 2013, pp. 1586-1592.
[26] S. D. Lin 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, pp. 1086-1090.
[27] Y. Gan and J. Zhong, "Image copy-move tamper blind detection algorithm based on integrated feature vectors," *Journal of Chemical and Pharmaceutical Research*, vol. 6, pp. 1584-1590, 2014.
[28] P. P. Panzade, C. S. Prakash, and S. Maheshkar, "Copy-move forgery detection by using HSV preprocessing and keypoint extraction," in *Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on*, 2016, pp. 264-269.
[29] T. Qazi, K. Hayat, S. U. Khan, S. A. Madani, I. A. Khan, J. Kołodziej, *et al.*, "Survey on blind image forgery detection," *IET Image Processing*, vol. 7, pp. 660-670, 2013.
[30] S. Sadeghi, S. Dadkhah, H. A. Jalab, G. Mazzola, and D. Uliyan, "State of the art in passive digital image forgery detection: copy-move image forgery," *Pattern Analysis and Applications*, pp. 1-16, 2017.
[31] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy–move forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 2284-2297, 2015.
[32] S. Dadkhah, M. Köppen, H. A. Jalab, S. Sadeghi, A. A. Manaf, and D. M. Uliyan, "Electromagnetismlike Mechanism Descriptor with Fourier Transform for a Passive Copy-move Forgery Detection in Digital Image Forensics," in *ICPRAM*, 2017, pp. 612-619.
[33] S. Sadeghi, S. Dadkhah, H. A. Jalab, G. Mazzola, and D. Uliyan, "State of the art in passive digital image forgery detection: copy-move image forgery," *Pattern Analysis and Applications*, vol. 21, pp. 291-306, 2018.
[34] H. Farid, "Photo Tampering throughout History " 2011.
[35] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic science international*, vol. 206, pp. 178-184, 2011.
[36] M. H. Al-Hammadi, G. Muhammad, M. Hussain, and G. Bebis, "Curvelet transform and local texture based image forgery detection," in *International Symposium on Visual Computing*, 2013, pp. 503-512.
[37] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding*, 2010, pp. 51-65.
[38] A. Myrna, M. Venkateshmurthy, and C. Patil, "Detection of region duplication forgery in digital images using wavelets and log-polar mapping," in *Conference on Computational Intelligence and*

Multimedia Applications, 2007. International Conference on, 2007, pp. 371-377.

[39] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, 2010, pp. 889-892.

[40] L. Zhou, D. Wang, Y. Guo, and J. Zhang, "Blur detection of digital forgery using mathematical morphology," in *Agent and Multi-Agent Systems: Technologies and Applications*, ed: Springer, 2007, pp. 990-998.

[41] J. Wang, G. Liu, B. Xu, H. Li, Y. Dai, and Z. Wang, "Image forgery forensics based on manual blurred edge detection," in *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, 2010, pp. 907-911.

[42] D.-Y. Hsiao and S.-C. Pei, "Detecting digital tampering by blur estimation," in *Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on*, 2005, pp. 264-278.

[43] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, pp. 180-189, 2007.

[44] H. Li and J. Zheng, "Blind Detection of Digital Forgery Image Based on the Edge Width," in *Intelligent Science and Intelligent Data Engineering*. vol. 7202, Y. Zhang, Z.-H. Zhou, C. Zhang, and Y. Li, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 546-553.

[45] J. Zheng and M. Liu, "A digital forgery image detection algorithm based on wavelet homomorphic filtering," in *Digital Watermarking*, ed: Springer, 2009, pp. 152-160.

[46] G. Ulutas and G. Muzaffer, "A new copy move forgery detection method resistant to object removal with uniform background forgery," *Mathematical Problems in Engineering*, vol. 2016, 2016.

[47] H.-D. Cheng, X. H. Jiang, Y. Sun, and J. Wang, "Color image segmentation: advances and prospects," *Pattern recognition*, vol. 34, pp. 2259-2281, 2001.

[48] M. Chen and S. A. Ludwig, "Color Image Segmentation Using Fuzzy C-Regression Model," *Advances in Fuzzy Systems*, vol. 2017, 2017.

[49] M. Brown, R. Szeliski, and S. Winder, "Multi-image matching using multi-scale oriented patches," in *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on*, 2005, pp. 510-517.

[50] D. G. Lowe, "Object recognition from local scale-invariant features," in *Computer vision, 1999. The proceedings of the seventh IEEE international conference on*, 1999, pp. 1150-1157.

[51] V. Ojansivu and J. Heikkilä, "Blur insensitive texture classification using local phase quantization," in *International conference on image and signal processing*, 2008, pp. 236-243.

[52] T.-T. Ng, S.-F. Chang, J. Hsu, and M. Pepeljugoski, "Columbia photographic images and photorealistic computer graphics dataset," 2005.