Blur Invariant Features For Exposing Region Duplication Forgery Using ANMS And Local Phase Quantization

Diaa M. Uliyan[1], Mohammed A. Fadhil Al-Husainy[2], Hesham Abusaimeh[3]
Faculty of Information Technology, Department of Computer Science, Middle East University, Amman, Jordan
Emails:diaa_uliyan@hotmail.com[1], dralhusainy@gmail.com[2], habusaimeh@meu.edu.jo[3]

Keywords: Image Forgery Detection, Image Forensics, Copy-Move Forgery, Region Duplication, Local Interest Points.

Received:

Abstract: *Recent researches have demonstrated that local interest points alone can be employed to faithfully detect region duplication forgery in image forensics. This type of forgery fully contained object with highly primitives such as corners and edges. Corners and edges represent the internal structure of any object in the image which makes them have a discriminating property under geometric transformations such as scale and rotation operation. They can be detected using Scale Invariant Features Transform (SIFT) algorithm. Here we provide an image forgery detection algorithm by using local interest points. Local interest points can be detected by extracting Adaptive non maximal suppression (ANMS) key points from dividing blocks in the image. We also demonstrate that ANMS key points can be effectively utilized to detect rotated and scaled forged regions. The ANMS features of the image are shown to exhibit the structure of copy-moved region. We provide a new texture descriptor called local phase Quantization (LPQ) that is robust to image blurring and also to eliminate the false positives of forged regions. Experimental results show that our method can detect region duplication forgery under scale, rotation and blurring of JPEG images on MICC-F220 and CASIA v2 datasets.*

1 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 [10], that seeing is no longer believing. Image forgery has inspired researchers [19] to investigate and check the authenticity of digital images due to its effect to the judgment of the truth of suspected images in many areas, such as digital newspapers, law evidences, medical documents, etc. Region duplication forgery is one of the most common image manipulation technique that is used for information abuse due to its simplicity and high visual impact. Furthermore, it is known as copy-move or cloning. 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.

Several methods have been developed to examine and locate Copy-moved regions in a forged image [6, 1]. About total 85 scientific research articles that cover the emerging topic "copy-move forgery detection", have been explored between 2007 and 2014 [41]. They are indexed in Web of Science as shown in Figure: 1. Some can detect duplicate regions [24, 35] and another can locate multiple duplicated regions [42]. The copy-moved detection methods have been categorized and evaluated based on their sensitivity towards two types of attacks: geometrical transformation operation attacks and post-processing attacks. For a geometrical transformation, the copy-move detection methods are resilient against spatial domain changes such as rotation [34], scale [13, 33] are evaluated. Conversely, some researchers have examined the robustness against the retouching and blending operation that reduces visual editing artifacts in the image through some post-processing attacks. Such attacks include blurring [40, 37], additive noise [31] and JPEG compression [18, 36] 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 and rotation attacks, as well as the mixture between the two in this research. Special scrutiny has granted to blur attack that has been highlighted by minor researchers [37]. As blurring could transform the features of any region in the image, further investigation of such attacks should be explored. The blur transformation in the image features may also make the performance of typical copy-move forgery detection methods [5] 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 [2] and CASIA v2.0 [8]. Then, the proposed method is implemented to combine the Scale Invariant Feature with LPQ matching technique. We then compare the performance of the proposed method by F-scores with three state-of-the-art methods: Amerini et al.'s method [2], Cozzolino et al.'s method [7], and Silva et al.'s method [32].

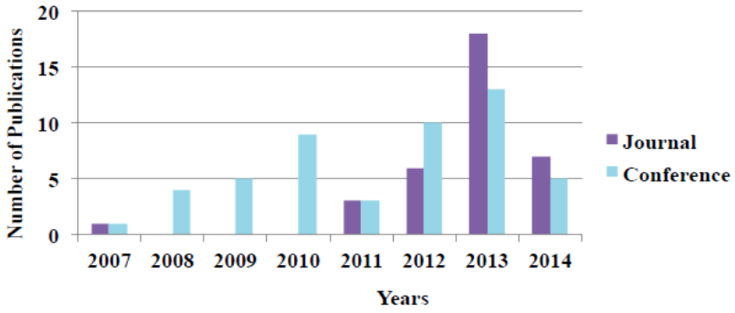


Figure: 1. Distribution of total number of Copy-move forgery detection papers per years.

This article is divided into five sections. Section 2 presents related works on copy-move forgery detection per some attacks included. Section 3 explains the proposed method. Section 4 discusses the experimental results and evaluation. Section 5 presents the conclusion and future works.

2 Related works

The common workflow of most copy-move forgery detection methods as shown in Figure: 2, have the following six steps: 1) image preprocessing, 2) image division, 3) feature extraction, 4) building descriptor 5) matching and 6) show detection results. The first step is optional, which tries to improve the image content by defeating undesired noise. The most frequent preprocessing step is image color conversion be converting an RGB color image into grayscale image [28] by using the Eq. 1.

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

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

Rafsanjany et al. [16] converts the input RGB image to Gray scale and Lab color space. Then, they divided it into square blocks to extract features. Their method achieved about 90% F-measure for JPEG images with size 512 x512. Another color conversion is used such as YC_bC_r color system to give the luminance information Y or chrominance information C_b and C_r [23]. Shinfeng et al. [20] used YC_bC_r color system for image conversion and divide it into blocks, for each block, DCT coefficients are extracted to produce 64 bit feature vector. Later, they compute the probability of each block by identifying the period of the it's histogram.

The main goal of the image conversion is to dimensionality reduction of the image features and extract the distinctive local interest points or visual features. This could help on performance the proposed copy-move forgery detection methods in the aspect of time complexity [12]. Similarly, Hue saturation Value (HSV) color space is used in Prajwal method [27] 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 two classes: block based methods [29], segmented based methods [35] and keypoint based methods [31]. In the block based method, the image is divided into a number of sub-blocks either square blocking or circle blocking. Similarly, segmented based method tries to segment the image into different regions that fully covered the forged objects in the image based on color, 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 minimize the time complexity for matching step 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 the exhibit the internal structure and its properties in the image. These features are saved into feature vector. Finally, matching between two feature vectors is employed using the distance of the nearest neighbor from all points in the feature space to show forged regions.

Regarding of development copy-move forgery detection steps, common methods focused on image division and feature extraction steps exhibit invariant features against geometric transformation and post processing attacks. Based on image division process, the Copy-move forgery detection methods are classified into: block-based, segmented-based and keypoint based methods are introduced as follows:

i. **Block based methods** divide the image into square or circle blocks to extract features from these blocks as shown in Figure: 3. The main advantage of this approach is that give high detection accuracy for the textured forged regions. But still gives high computational complexity due to exhaustive search between divided blocks in the image.
ii. **Segmented based methods** Segment the image into homogenous regions based on color or texture. This approach works well in the forged images that have duplicated objects.

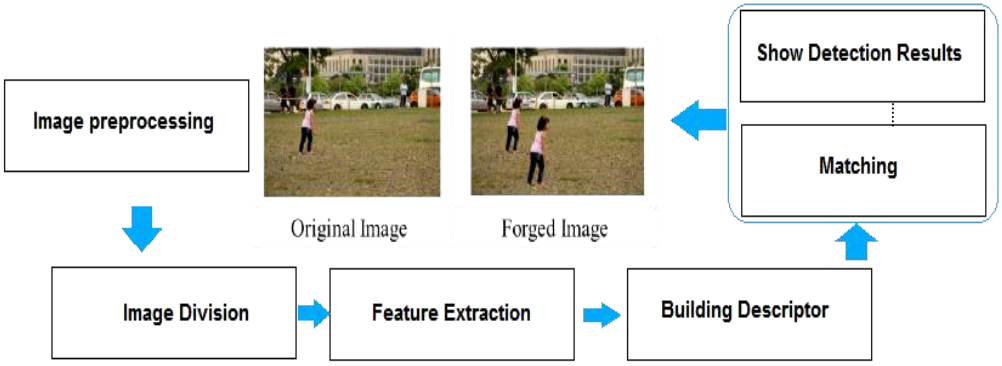


Figure: 2. The common framework of the copy-move forgery detection methods [31].

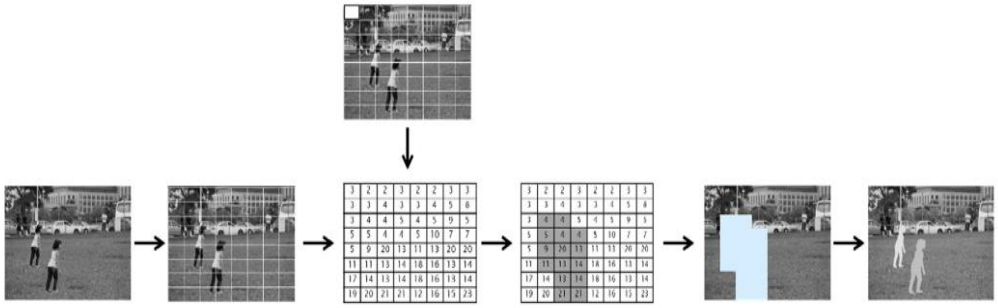


Figure: 3. The image is divided into 8 x8 blocks, features are highlighted and saved for matching process .

iii. **Keypoint based methods** discard block division step and use local interest point detector 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 a reliability against geometric transformation attacks [9].

Different types of attacks have been considered in existing methods for detecting region duplication forgery. These metods are called Passive methods due to detecting image forgery without requiring explicit prior information. The main goal is to analyze the history of the image tampering blindly by examining pixel-level correlations [11].

In this article, popular feature extraction methods in copy-move forgery detection methods were covered for various geometric transformations and post processing attacks. The robustness of detection methods depends on invariant features to possible attacks as pointed in [6]. Copy-move forgery detection methods based on type of features are classified into two classes : Frequency transform methods [15], Texture and intensity based methods [36].

i. **Frequency transform methods** convert the image pixel information into frequency domain to extract high frequency coefficients form the image. This approach is robust to JPEG compression and can detect duplicated regions with a large size 128 x 128 pixels. The limitations are the high computational complexity and struggle to detect duplicated regions with scale and rotation attacks. The frequrncy features are: Discrete cosine transform (DCT), Fourier Transform (FT), Discrete wavelet transform (DWT), Curvelet Transform (CT) and Wiener Filter. The limitation of this approach is sensitivity to blurring attacks.

ii. **Texture and intensity based 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 such as Local binary Patterns (LBP), Histogram of Gradient (HOG), Zernike moments (Zm) [30] which is robust to rotation, log polar transform [25] that detects rotated duplicated regions, Principle 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 utilize frequency and texture features fall in scope of 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 Keypoint based approach such as Scale invariant transform features (SIFT), speed up robust features (SURF) [3] and Harris features. These features are slightly blur invariant. This motivates us to develop a blur invariant detection method to detect blurred forged regions in the image.

blurring is made effectively through image forgery process suing averaging of neighbor pixels in a square block [44]. 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 it's simplicity. If the duplicated region is retouched by blur, then the main features of the blurred region are minimized and details cannot be seen. Blurring on forged regions aims to manipulate region's information and assists hidding retouch and blending artifcats. As a result, blurring allow the duplicated region to be consistent with its surrounding area. The scope of locating tampered regions attacked by blurring artifact is even smaller. Only few relevant research papers have been discovered that deal with blur attack [14, 22, 44, 39, 17, 40].

The first attempt was made by Mahdian and Saic [22] to detect burred 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. But it still struggles to detect uniform duplicated regions and gives high false positives. Another blur detection method is developed by Zhou et al. [44] for detecting blurred edges in the duplicated regions. Their method starts by preprocessing step to convert the image into binary image. 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 about 89.26% in images with blurred edges manually attacked by the Gaussian noise filter. Zheng and Liu [43] located tampered regions with blur attack based on wavelet homomorphic filters to improve the high frequency edges. Then, erosion operation was applied to expose blurred edges from normal ones which effectively reduced the false positive rates. Wang et al. [39] used non subsampled contourlet transform (NCST) to examine manually blurred edges from duplicating regions. The detection of forged duplicated regions is done using support vector machine (SVM). In [40], blur artifacts were explored in forged regions by using combined blur and affine transform moments. The relative detection error was employed as a measure of the stability of invariant features distorted by motion and Gaussian blurs. The method achieved high accuracy rate with small feature dimension. Guzin et al. [38] 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 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.

In this paper, a robust region duplication forgery detection method using ANMS keypoints and LPQ texture descriptor. Region duplication is one of the widely used techniques for image forgery. In this paper, a portion of the image is copied and pasted to another region of the same image to hide the original content and change the semantic meaning of the image. While copy-move operation is applied, the duplicated region may post processed using rotation, scaling, blurring to create better forgery. The common pipeline of the proposed method is, first the input image is segmented based on color features. 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. These Keypoints are scale and translation invariant features. Second, each segment is divided into 4 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. The extracted features are scaled and blur invariant. The closest point search of features between two segments is applied using Generalized Nearest neighbor (G2NN) to improve the performance of our method in terms of True positive rate (TPR) and false positive rate (FPR).

3 Proposed method

In this section, we introduce in detail the flowchart of the proposed method for exposing 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: 4.

3.1 Image Preprocessing

Image segmentation is the one of the most important techniques for image analysis and object detection. 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 divide an image into homogeneous regions 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 color segmentation approach, followed by Fuzzy C-means (FCM) clustering algorithm introduced in [5]. The fuzzy C-means is an unsupervised technique which compares the RGB channel of every pixel in the image with the centroid of the cluster. It makes a decision about which category the pixel should relate to. Each pixel in the image should have a value between 0 and 1 that 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 should be the value 1. The FCM clustering is an iterative optimization that minimizes the cost function described as follows:

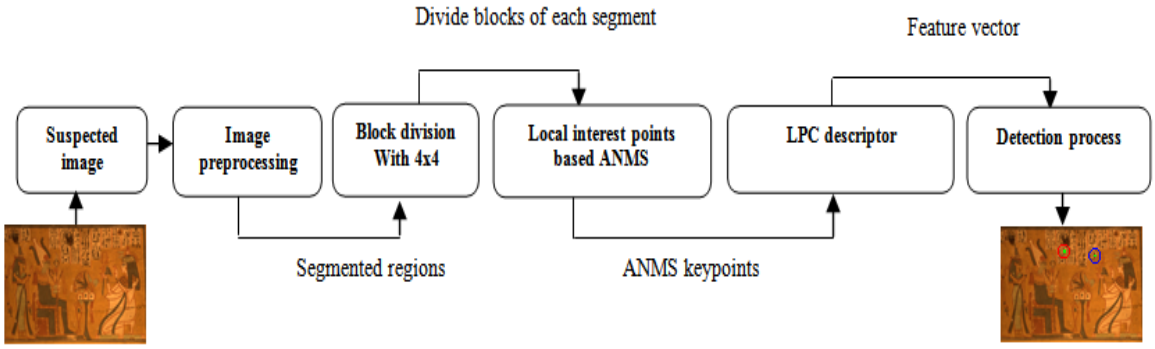


Figure: 4. Main steps of our copy-move forgery detection technique.

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

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 are 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 is the centroid of the k^{th} cluster and $|p_i - v_k|$ is the Euclidean distance between p_i and v_k.

By using the cluster information (c=5, maximum number of iterations=10) and the pixels information pi from the forged image I with size 512 x 512, the homogenous regions including copy-moved regions can be extracted as shown in Figure: 5.

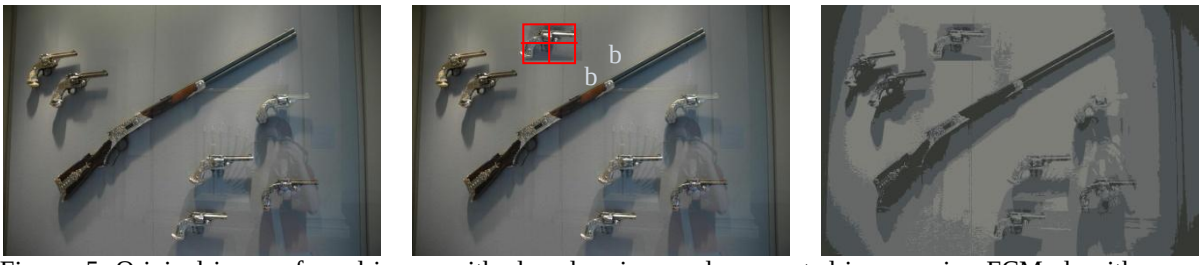


Figure: 5. Original image, forged image with cloned regions and segmented image using FCM algorithm are listed respectively.

Consequently, each segment is divided into 4 non overlapping blocks of $b \times b$ pixels, where $b = 4$ as shown in Figure: 5. We introduce below, the process of extracting features from these blocks to exhibit the internal structures of segments and achieve rotation invariance.

3.2 Adaptive non maxima suppression (ANMS) features

Keypoints based methods are significantly helpful in detecting visual objects in the image. While the block-based methods divide the image into blocks, keypoint based methods identify and highlight only regions with high entropy, called the local interest points or keypoints. However, keypoints such as SIFT are robust against geometric transformations such as scaling. But major drawback is that keypoints may be insufficient or even none in the forged region of uniform texture. To avoid the drawback in SIFT based methods, we adopt the ANMS method which is an effective approach suggested by Brown, Szeliski, & Winder [4] to select uniformly distributed interest points $K = \{K1, , K2, \dots, K_m | K \in (\mu_{K_m}, V_{K_m})\}$ 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 Eq. 4:

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

Where w(x,y) is a Gussian kernel defined below, and (u,v) is the minimal Euclidean distance.

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

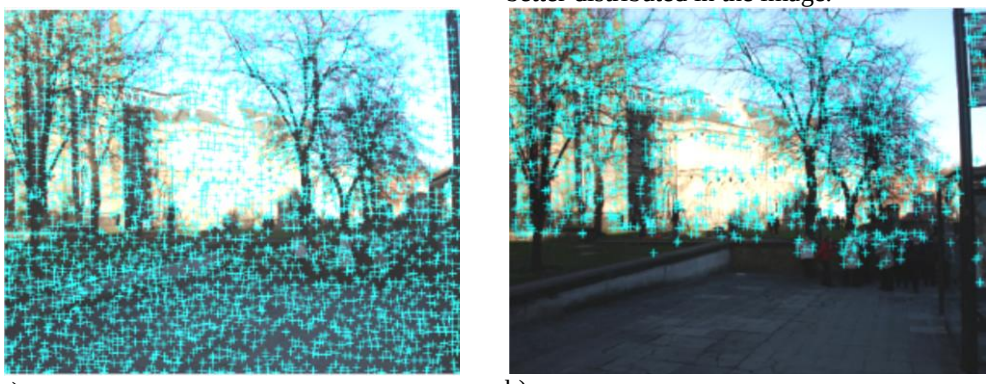
Where σ is the Standard Deviation. Then, Taylor series expansion is employed to the Eq. of $E(\mu, v)$ to eliminate the weak interest points as follows

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

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: 6 shows the results obtained by the ANMS compared with the SIFT based method [21]. ANMS points are much better distributed in the image.



a) b)

Figure: 6. Keypoints detected by a) ANMS method and b) SIFT method.

3.3 Local Phase (LPQ) descriptor

Ojansivu et al. [26] 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 point spread function (PSF) as follows

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

Where, where g(x, y) denotes 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.

In terms of frequency domain, the Eq. 8 is converted to:

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

Where G(u,v), F(u,v) and H(u,v) dentote to the discrete Fourier transforms (DFT) of the blurred PSF image g(x,y), the original image f(x,y), and the PSF h(x,y), respectively. u,v are frequency coefficients in the blurred image. After the Fourier transform , the image has 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 valued parts are quantized based on scalar quantizer as follows

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

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

Finally, LPQ descriptor, which is similar to Local binary pattern (LBP) [36], and is calculated as follows

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

In Figure: 7, an example of the computing LPQ for sample images from CASIA dataset and the duplicated regions are clearly recognized.

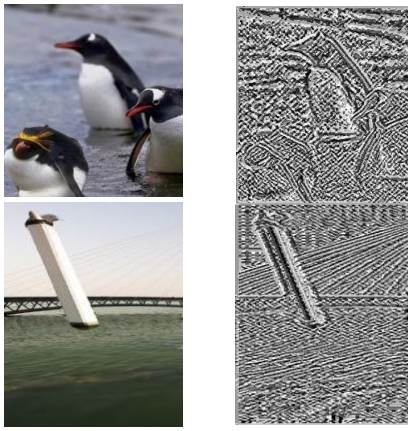


Figure: 7. LPQ descriptor of sample images on CASIA v2.

3.4 Forgery localization process

As discussed above, keypoints for each segmented region are extracted by ANMS. The LPC descrciptor 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 generalized nearest neighbor (G2NN) [2]. 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 Eucledian Distance, T is threshold value=0.5 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 keypoints, simply evaluate the distance between two descriptors with respect to a global threshold *T*.

4 Experimental results

The performance of the blur invariant detection method was examined through a set of image forgery. Firstly, we introduce the experimental setup of our method and performance evaluation metric used in detecting duplicated regions. Then, the proposed method is compared with the methods developed in [2], [7], and [32].The details of the experiments are discussed below.

Our method is developed by MATLAB R2014a on Intel Core i5 processor, with 16 GB memory. The forged images were collected from the dataset MICC-f220 and CASIA v2 which have about 510 images with size vary from 240×160 to 900×600 pixels. A duplicated region on an image was copied and moved with the simple transformation attacks comprising scaling, rotation and blurring. The evaluation metric is defined to include: True positive (TP), True negatives (TN), False positives (FP), False negatives (FN) and F-score calculated as follow:

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

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

Various scaling transformations have been applied for images (A-C) in the MICC-F220 dataset. Where Sx and Sy are scaling factors applied to the x and y axis of the tampered image part as shown in Figure: 8.

Some experiments for JPEG compressions are addressed. The performance of our method is evaluated in set of images compressed with various quality factors (QF=80,70,50) 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.

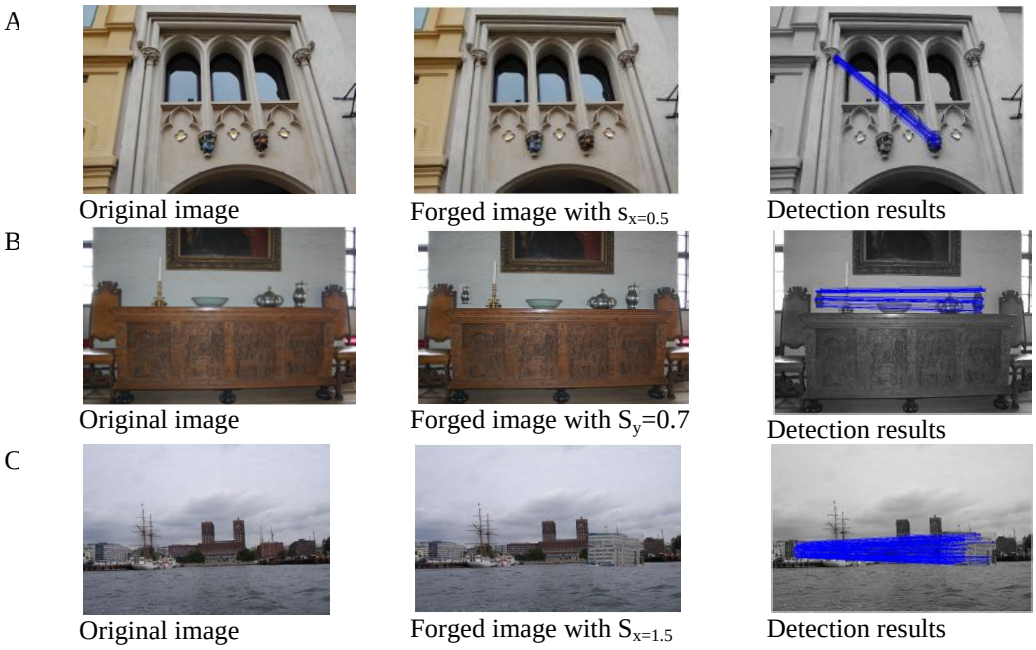
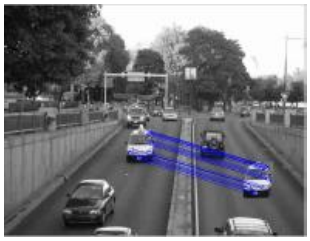
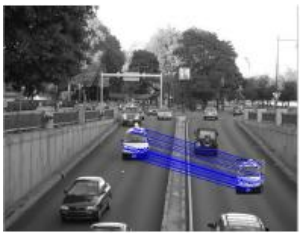


Figure: 8. Detection of scaled duplicated regions in forged images.

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



c) Detection results with QF=70



d) Detection results with QF=80

Figure: 9. The robustness of the proposed method against JPEG compression

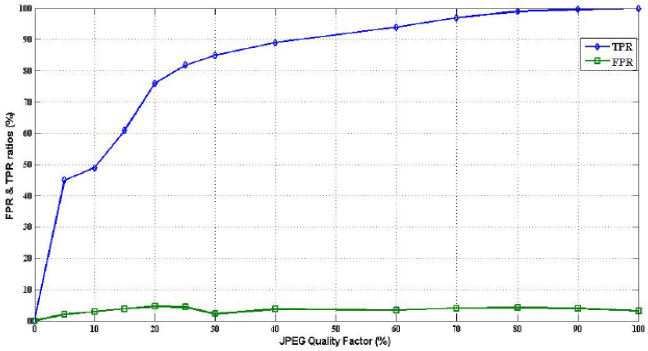


Figure: 10. ROC curve of the proposed method in terms of TPR and FPR on MICC-F220

In this part, some experiments of copy move forgery under blur manipulations with their corresponding descriptors constructed by our method. Here, we use Gaussian blurs with radius varying from 0.5 to 2. The details are shown in Figure: 11.

The performance of the proposed method in terms of TP, FP and F-score compared with others is shown in Table. 1.

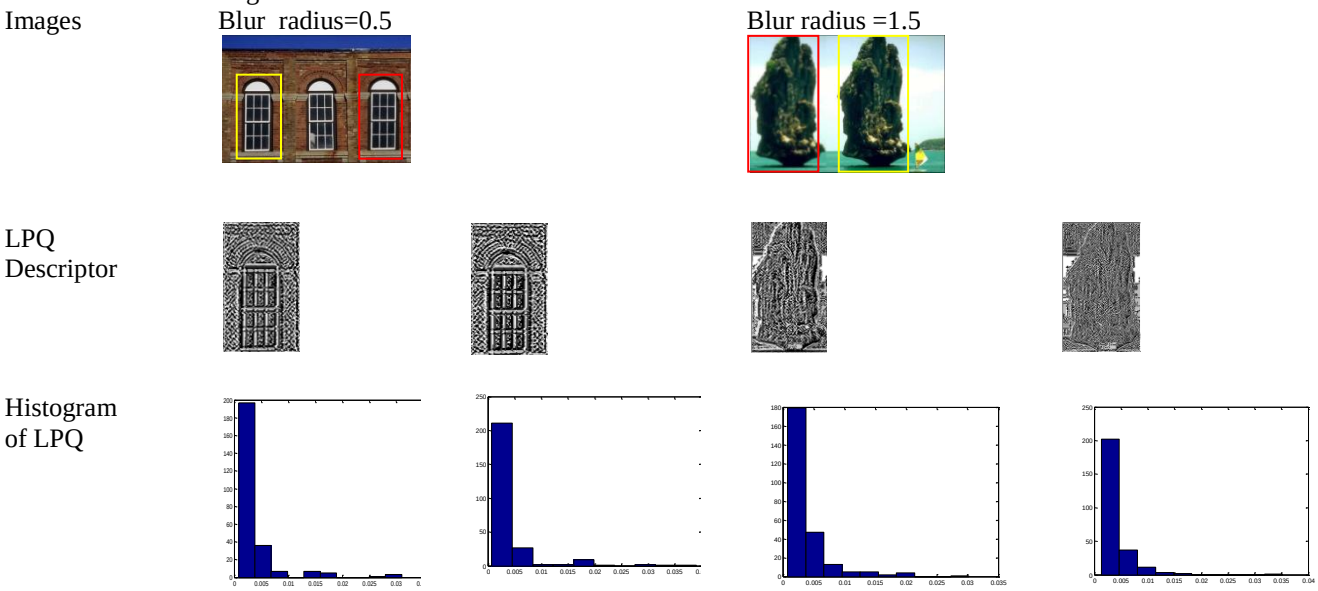


Figure: 11. Robustness of the proposed method under Gaussian blurring on CASIA v2.

Table. 1 performance of our method compared with existing methods			
Methods	**TP**	**FP**	**F-score**
***Amerini et al.* [2]**	22	7	0.114
***Cozzolino et al.* [7]**	147	1	0.786
Silva et al.* *[32]	46	15	0.229
Our method	165	5	0.84

5 Conclusion

In this paper, robust features 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 color segmentation has reduced the FP in the image. Clustering segments based on fuzzy C means increases the TP of matching the duplicated regions over ANMS keypoints matching. From the suspected forged image, the proposed method can find the duplicated regions, even if they are post processed by geometrical transformations like scaling or blurring. Future works will focus on image forgery with reflections and illumination change.

References

[1] Al-Qershi, O. M. and B. E. Khoo (2013). "Passive detection of copy-move forgery in digital images: State-of-the-art." Forensic science international **231**(1): 284-295.

[2] Amerini, I., L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra (2011). "A sift-based forensic method for copy–move attack detection and transformation recovery." Information Forensics and Security, IEEE Transactions on **6**(3): 1099-1110.

[3] Bo, X., W. Junwen, L. Guangjie and D. Yuewei (2010). Image copy-move forgery detection based on SURF. Multimedia Information Networking and Security (MINES), 2010 International Conference on, IEEE.

[4] Brown, M., R. Szeliski and S. Winder (2005). Multi-image matching using multi-scale oriented patches. Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on, IEEE.

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

[6] Christlein, V., C. Riess, J. Jordan and E. Angelopoulou (2012). "An evaluation of popular copy-move forgery detection approaches."

[7] Cozzolino, D., G. Poggi and L. Verdoliva (2015). "Efficient dense-field copy–move forgery detection." IEEE Transactions on Information Forensics and Security **10**(11): 2284-2297.

[8] D. Jing, W. W. (2011). "CASIA Tampered Image Detection Evaluation (TIDE) Database."

[9] Dadkhah, S., M. Köppen, H. A. Jalab, S. Sadeghi, A. A. Manaf and D. M. Uliyan (2017). Electromagnetismlike Mechanism Descriptor with Fourier Transform for a Passive Copy-move Forgery Detection in Digital Image Forensics. ICPRAM.

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

[11] Farid, H. (2011). "Photo Tampering throughout History ".

[12] Gan, Y. and J. Zhong (2014). "Image copy-move tamper blind detection algorithm based on integrated feature vectors." Journal of Chemical and Pharmaceutical Research **6**(6): 1584-1590.

[13] Guo, J.-M., Y.-F. Liu and Z.-J. Wu (2013). "Duplication forgery detection using improved DAISY descriptor." Expert Systems with Applications **40**(2): 707-714.

[14] Hsiao, D.-Y. and S.-C. Pei (2005). Detecting digital tampering by blur estimation. Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on, IEEE.

[15] Huang, Y., W. Lu, W. Sun and D. Long (2011). "Improved DCT-based detection of copy-move forgery in images." Forensic science international **206**(1): 178-184.

[16] Kushol, R., M. S. Salekin, M. H. Kabir and A. A. Khan (2016). Copy-Move Forgery Detection Using Color Space and Moment Invariants-Based Features. Digital Image Computing: Techniques and Applications (DICTA), 2016 International Conference on, IEEE.

[17] Li, H. and J. Zheng (2012). Blind Detection of Digital Forgery Image Based on the Edge Width. Intelligent Science and Intelligent Data Engineering. Y. Zhang, Z.-H. Zhou, C. Zhang and Y. Li, Springer Berlin Heidelberg. **7202:** 546-553.

[18] Li, X.-h., Y.-q. Zhao, M. Liao, F. Shih and Y. Shi (2012). "Passive detection of copy-paste forgery between JPEG images." Journal of Central South University **19**(10): 2839-2851.

[19] Li, Y. (2012). "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching." Forensic science international.

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

[21] Lowe, D. G. (1999). Object recognition from local scale-invariant features. Computer vision, 1999. The proceedings of the seventh IEEE international conference on, Ieee.

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

[23] Muhammad, G., M. H. Al-Hammadi, M. Hussain, A. M. Mirza and G. Bebis (2013). Copy move image forgery detection method using steerable pyramid transform and texture descriptor. EUROCON, 2013 IEEE, IEEE.

[24] Muhammad, G., M. Hussain and G. Bebis (2012). "Passive copy move image forgery detection using undecimated dyadic wavelet transform." Digital Investigation **9**(1): 49-57.

[25] Myrna, A., M. Venkateshmurthy and C. Patil (2007). Detection of region duplication forgery in digital images using wavelets and log-polar mapping. Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on, IEEE.

[26] Ojansivu, V. and J. Heikkilä (2008). Blur insensitive texture classification using local phase quantization. International conference on image and signal processing, Springer.

[27] Panzade, P. P., C. S. Prakash and S. Maheshkar (2016). Copy-move forgery detection by using HSV preprocessing and keypoint extraction. Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on, IEEE.

[28] Peng, F., Y.-y. Nie and M. Long (2011). "A complete passive blind image copy-move forensics scheme based on compound statistics features." Forensic science international **212**(1): e21-e25.

[29] Qazi, T., K. Hayat, S. U. Khan, S. A. Madani, I. A. Khan, J. Kołodziej, H. Li, W. Lin, K. C. Yow and C.-Z. Xu (2013). "Survey on blind image forgery detection." IET Image Processing **7**(7): 660-670.

[30] Ryu, S.-J., M.-J. Lee and H.-K. Lee (2010). Detection of copy-rotate-move forgery using Zernike moments. Information Hiding, Springer.

[31] Sadeghi, S., H. A. Jalab, K. Wong, D. Uliyan and S. Dadkhah (2017). "Keypoint based authentication and localization of copy-move forgery in digital image." Malaysian Journal of Computer Science **30**(2): 117-133.

[32] Silva, E., T. Carvalho, A. Ferreira and A. Rocha (2015). "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes." Journal of Visual Communication and Image Representation **29**: 16-32.

[33] Uliyan, D. M. and M. A. Al-Husainy (2017). "Detection of Scaled Region Duplication Image Forgery using Color based Segmentation with LSB Signature." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS **8**(5): 126-132.

[34] Uliyan, D. M., H. A. Jalab, A. W. Abdul Wahab and S. Sadeghi (2016). "Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points." Symmetry **8**(7): 62.

[35] Uliyan, D. M., H. A. Jalab, A. Abuarqoub and M. Abuhashim (2017). Segmented-Based Region Duplication Forgery Detection Using MOD Keypoints and Texture Descriptor. Proceedings of the International Conference on Future Networks and Distributed Systems, ACM.

[36] Uliyan, D. M., H. A. Jalab and A. W. A. Wahab (2015). Copy move image forgery detection using Hessian and center symmetric local binary pattern. Open Systems (ICOS), 2015 IEEE Confernece on, IEEE.

[37] Uliyan, D. M., H. A. Jalab, A. W. A. Wahab, P. Shivakumara and S. Sadeghi (2016). "A novel forged blurred region detection system for image forensic applications." Expert Systems with Applications **64**: 1-10.

[38] Ulutas, G. and G. Muzaffer (2016). "A New Copy Move Forgery Detection Method Resistant to Object Removal with Uniform Background Forgery." Mathematical Problems in Engineering **2016**.

[39] Wang, J., G. Liu, B. Xu, H. Li, Y. Dai and Z. Wang (2010). Image forgery forensics based on manual blurred edge detection. Multimedia Information Networking and Security (MINES), 2010 International Conference on, IEEE.

[40] Wang, T., J. Tang and B. Luo (2013). Blind detection of region duplication forgery by merging blur and affine moment invariants. Image and Graphics (ICIG), 2013 Seventh International Conference on, IEEE.

[41] Warif, N. B. A., A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband and K.-K. R. Choo (2016). "Copy-move forgery detection: Survey, challenges and future directions." Journal of Network and Computer Applications **75**: 259-278.

[42] Zhao, J. and J. Guo (2013). "Passive forensics for copy-move image forgery using a method based on DCT and SVD." Forensic science international **233**(1): 158-166.

[43] Zheng, J. and M. Liu (2009). A digital forgery image detection algorithm based on wavelet homomorphic filtering. Digital Watermarking, Springer**:** 152-160.

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