Expert Systems With Applications 64 (2016) 1–10

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

A novel forged blurred region detection system for image forensic applications

Diaa M. Uliyan, Hamid A. Jalab*, Ainuddin W. Abdul Wahab, Palaiahnakote Shivakumara, Somayeh Sadeghi

Faculty of Computer Science and Information Technology, Multimedia Unit, University of Malaya, 50603 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 6 May 2016
Revised 18 July 2016
Accepted 19 July 2016
Available online 19 July 2016

Keywords:
Copy–move detection
Blurred forged region detection
Statistical features
Phase congruency
Structural features,
feature similarity

ABSTRACT

As new technologies and devices are introduced in the market, the crime rate also increases in developing and developed countries. One such crime is image forgery which can be detected by forensic applications. In this paper, we propose a novel idea for identifying forgery attack done by blur artifact unlike existing forgery attack done by geometrical distortion such as rotation and scaling. The proposed method segment region of interest from the input forgery image based on the combination of statistical analysis with color texture analysis which includes blur artifact region. For each region of interest, we propose a new method for estimating degree of blur to separate forged blur artifact and normal blur artifact. In order to validate the identified forged blur artifact, we explore Fourier and Gabor texture features to study the structure of the forged blur artifact which eliminates false blur forged blur artifact. To evaluate the proposed forged blurred region detection method, we use two standard databases namely, Image data manipulation, and MICC-F220 for experimentation. Experimental results of the proposed method with existing methods show that the proposed method outperforms the existing methods in terms of forged blur artifact region detection.

1. Introduction

With the rapid development of digital image technology, digital images have been integrated into all aspects of daily life. As a result, high-resolution digital cameras and modern image-editing tools such as Photoshop have made the image tampering more easier. Image manipulation methods are classified into image tampering or image steganography. Both image tampering and steganography are manipulate a digital image but, they differ from each other according to their purposes. Steganography manipulates an image for the purpose of hidding secret information whereas the image tampering changing an image to achieve twisted objectives.

There have been a huge amount of steganographic embedding algorithms using digital images as hosts for covert communication (Kessler, 2004). However, in the same time, numerous steganalysis algorithms have been used to find the hidden data in digital images (Almohammad, Hierons, & Ghinea, 2008). Embedded information, such as secret messages, is restored during the authentication step through comparison with reference data. The authentication information is then used to verify whether the digital media has been forged in forensic investigations or not (Almohammad et al., 2008; Almohammad, Ghinea, & Hierons, 2009; Rao & Babu, 2016).

As pointed by Hayati, P., and Chang (2007), many of existing steganography tools have been used to help digital forensic investigators in their multimedia analysis. Forensic means finding evidence to solve a crime, and e-Forensics means the process of finding electronic evidence in a manner that is legally suitable to solve a crime (Potdar, Khan, Chang, Ulieru, & Worthington, 2005). Steganography and steganalysis are now equally standard concept in information security (Ker et al., 2013).

Digital images can be tampered very easily due to availability of many powerful image editing softwares. For example, forged images in digital newspapers mislead the public and falsify truths as an important object may be duplicated or removed from images. In this way, we can find several image tampering detection methods for forensics applications (Al-Qershi & Khoo, 2013; Christlein, Riess, Jordan, & Angelopoulou, 2012). One such example is illustrated in Fig. 1 where (a) is the original image, (b) is the forged one where the one soldier is removed from the image and (c) is the suspicious regions identified by the method (Mahdian & Saic, 2007) which works based on identifying blur moments. It is noticed from Fig. 1(b) that since the person is removed by the devices, it introduces some sort of distortions, such as blur, noise,

* Correspondence author.
E-mail addresses: diaa_uliyan@hotmail.com (D.M. Uliyan), hamidjalab@um.edu.my (H.A. Jalab), ainuddin@um.edu.my (A.W.A. Wahab), shiva@um.edu.my (P. Shivakumara), ssomayeh@siswa.um.edu.my (S. Sadeghi).

http://dx.doi.org/10.1016/j.eswa.2016.07.026
0957-4174/

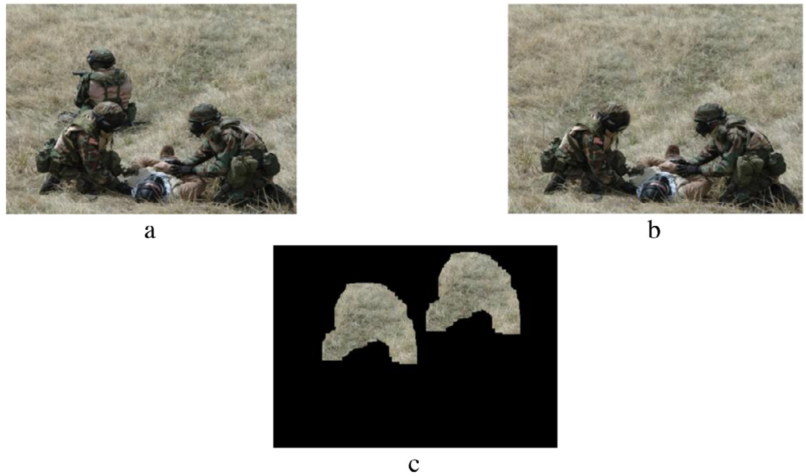

Fig. 1. (a) The original image (b) The forged image (c) The detection result of method (Mahdian & Saic, 2007).

degradations, etc. Based on this evidence, the method in (Mahdian & Saic, 2007) identifies successfully the regions as suspicious. We can notice from Fig. 1(b) that our vision system definitely fails to identify the suspicious regions without original image. In the same way, one can expect forged image may contain duplicate objects brought from the same image which is called copy-move forgery. This shows that identifying forgery is hard, and hence, it has become a major topic for the researchers in recent days (Huang, Lin, Hu, & Chou, 2014; Kakar & Sudha, 2012).

The solution for identifying tampered information in image is not a new problem according to literature. We can find several forgery detection methods in literature that can be classified as active methods (Huo, He, & Chen, 2013; Li, He, Huang, & Shi, 2011; Singh & Ranade, 2013) and passive methods (Birajdar & Mankar, 2013; Lin, Wang, & Kao, 2009; Piva, 2013).

In active method, mainly watermarking and steganography techniques are used to embed the digital authentication information into the original image(Guo, Liu, & Wu, 2013). The authentication information may be used as a verification for forensic investigation when the image has been falsified. The limitation of this technique is that it needs special cameras or subsequent processing of the digital image. Furthermore, some watermarks may distort the quality of the original image. Due to these restrictions, the researchers tend to develop passive techniques for digital image forensic.

Passive image forensics approache is proposed as a new image forgery detection method without requiring explicit prior information (Al-Qershi & Khoo, 2013; Birajdar & Mankar, 2013).

The passive method can be classified further into two categories: First, the methods that use camera parameters for identifying forged image(Kang, Li, Qu, & Huang, 2012; C.-T. Li, 2010). These methods try to identify the camera if the forged image is captured by different devices or camera. The second category methods are developed which work based on analyzing the local information to find suspicious region in the image based on distortion introduced by copy-move process (Christlein et al., 2012; Shao, Yu, Xu, & Cui, 2012; Zhang, Wu, Wang, You, & Wang, 2010).

Copy–move forgery is becoming one of the most popular image tampering. Copy–move forgery is copying a region of an image and pasting it in another location of the same image. The key characteristic of the duplicated regions is that they have the same noise components, textures, color patterns, homogeneity conditions and internal structures. The forgers perform duplicate regions with different geometric and post-processing operations to hide traces and make consistency with surrounding area.

Hence, image forgery may cause troubles to digital content provider. Most of image forgeries try to blur forged regions to reduce the discontinuity of their boundaries caused by copy move operation (Liu, Wang, Lian, & Dai, 2013; Sheng, Gao, Cao, Gao, & Fan, 2012).

In this study we focus on identifying forgery attack done by blurring to detect tampered images. Blurring could happen on object in the image to make it consistent with the rest of image. As a result, experienced investigators cannot examine the trustworthiness of such images visually. It is still a challenging matter to carry out the automatic detection by computer. The detection of blurred region duplication forgery has become an essential need for image forensics. In this paper, blurred cloned regions are considered and the corresponding region duplication detection method is introduced. This paper is organized as follows: Section 2 presents the related work. Section 3 describes the proposed method. Sections 4 and 5 present the experimental results and conclusion.

2. Related work

The simple blur operation is effectively based on the mathematical averaging of neighbor pixel values in a sliding square window (Zhou, Wang, Guo, & Zhang, 2007). Three types of blur are common: Gaussian, defocus, and motion blurs (Shan, Jia, & Agarwala, 2008). In practice, the use of the Gaussian blur filter during image forgery is regarded as simple and effective. If the image region is blurred after the copy–move forgery process, then the main intentional features of the blurred region are reduced and details cannot be perceived. Blurring of duplication image regions is a common process in image manipulation which help to hide traces and make consistency with surrounding area. The field of identifying tampered information attacked by blur artifact is even smaller. Only few relevant publications have been found.

The authors Mahdian and Saic, (2007) proposed blur invariant moments method to extract the features from image blocks for copy move forgery detection. The method used principal component transformation to reduce the dimension of the blocks representation, and a k–d tree is used for detecting the duplicated regions. Due to the problem with uniform areas in images, this method suffers from high false detections for localization of tampered areas.

A new blur edge detection method is proposed by Zhou et al. (2007) for detecting duplicated regions in the presence of blur attack by exploring the blurred edges of interested regions. The method starts by converting the image into binary image. Then, edge preserving–smoothing filters are applied to the binary image, followed by a mathematical morphology process based on erosion operation to detect forged regions with manual blurred edges. The average detection rate was 89.26% using images collected from the Internet, and images are blured manualy with Gaussian blur filter.

Another detection method based on blur as a clue is proposed by Zheng and Liu, (2009). This method localized forged regions in the presence of blur operation using wavelet homomorphic filtering to enhance the high frequency edges after the blurring process. The method used erosion operation to enhance blurred edges from regular ones which effectively reduced the detecting errors.

An effective image forensics method is proposed by Wang et al. (2010) for classification of forged duplicated regions based on non-subsampled contourlet transform (NCST). In contrast with the traditional homonorphic filtering, the non-subsampled contourlet transform has enhanced the forged regions by exposed the existence of manual blurred edges from duplicated regions in forged image. The classification of forged duplicated regions is done using support vector machine (SVM).

The identifying tampered regions attacked by blur artifact was also discussed by (Wang, Tang, & Luo, 2013), in which the detected blurred duplicate regions achieved by using four combined blur and affine moments to extract features of blocks. In this method, relative error was utilized as a measure of the stability of invariant features distorted by motion and Gaussian blurs. The method achieved high detection rate with lower feature dimension.

When we look at review of the above methods, we can observe that the degree of blur amounts which is used to identify the blurred tampered regions is ignored by these methods. In other words, the methods are not capable of handling different blurred attacks. Therefore, in this study, we propose a novel method for detecting forged region attacked by blur artifact. The main contributions of this study are as follows: (1) Exploring statistical analysis with color texture for segmenting region of interest from the image. (2) Use of blur metric to estimate degree of blur in the region of interest and (3) Combining intensity and orientation information by Fourier and Gabor to detect tampered blurred region from the blur regions.

3. Proposed method

As discussed in introduction and related work sections, forgery can be made in many ways to confuse the methods. The recent forgery attack is making forged or duplicate regions blur to create confusion with other blurred regions and non-blurred regions. For such input forged image, first, we propose to segment the region of interest in the image which includes forged blurred region also because it is a forged region by a copy-move process. It is true that each object in the image have high contrast value compared to its background since it is defined as object. As a result, we can expect high contrast values at edges and near edges. Besides, we can also expect uniform texture throughout the object. With these notions, we propose statistical analysis and color texture to segment the region of interest (ROI). Since forged blurred region is also an object, it is classified as region of interest. Next, we propose blur metric to estimate degree of blurred regions from the region of interest. This results in blurred and non-blurred region of interest. Due to camera motion or object motion, there are chances of introducing blur in the images which may results in actual blurred regions. To separate forged blurred region from actual blurred region, we propose a new idea of combining Fourier coefficients and gradient based features because it is fact that Fourier high frequency coefficients and gradients are not much sensitive to blur as intensity values and edges. The features are matched with predefined samples to identify forged blurred region. The pipeline of the proposed method can be seen in Fig. 2.

3.1. Segmenting region of interest (ROI)

Based on the similarity of the internal structure of duplicated regions, the input image is segmented into homogenous regions. Segmentation of the image is carried out using SRM algorithm to capture the main objects in the image using effective statistical image analysis (Nock & Nielsen, 2004).

For input image, I that contains $|I|$ pixels, the proposed method obtains R, G and B color spaces where each of the three values belongs to the set $(1, 2, \ldots, g_n)$. Each color space is represented by an eight-bit image, $g_n = 256$. In order to segment the region of interest, the proposed method finds uniform color R in each space as denoted by $b(R)$.

$$b(R) = g_n\sqrt{\frac{1}{2Q|R|} In \frac{|S_{|R|}|}{\delta}}, \quad (1)$$

Where $\delta = \frac{1}{(6|I|^2)}$ is a probability error with a small value. It is inversely proportional to the square of the size of image I to limit over segmentation in the mapped image. $S_{|R|}$ denotes the set of regions with $|R|$ pixels, and Q is in the range [1–256]. To merge neighbor regions, say R and R' with color averages, $|\bar{R}_a|$ and $|\bar{R}'_a|$ for channel a, respectively, it can be given as:

$$P(R, R') = \begin{cases} true & if\ \forall a \in \{R, G, B\}, \\ & |\bar{R}'_{a-}\bar{R}_a| \le \sqrt{b^2(R') + b^2(R)}, \\ false & else \end{cases} \quad (2)$$

If $P(R, R')$ is true, then R and R' can merge into a large region.

The process of segmentation step is illustrated in Fig. 3 where (a) is the result by the segmentation step which shows the region of interest segmented from the background, (b) indicates that the forged blurred region is also included in the region of interest in Fig. 3(a).

3.2. Blurred region detection

To differentiate between normal and blurred regions within a single image, we predict the blur degree for each region based on the perceptual blur metric model presented in Crete, Dolmiere, Ladret, & Nicolas, (2007). The algorithmic steps of the blurred region detection are as follows.

Step 1: Horizontal and vertical low pass filters H_{hor} and H_{ver} are applied to each region I_{reg} with size $m \times n$. Blurred regions B are obtained as follows:

$$B_{ver} = I_{reg} * H_{ver}\ ,\ \ B_{hor} = I_{reg} * H_{hor} \quad (3)$$

Where | * | denotes the convolution operator.

Step 2: The horizontal and vertical absolute differences between the original region and its blurred vision are computed. These image differences are expressed as follows:

$$D_{Iver}(i, j) = \sum_{i=1}^{m-1}\sum_{j=0}^{n-1} |I_{reg}(i, j) - \ I_{reg}(i-1, j)|$$

$$D_{Ihor}(i, j) = \sum_{i=0}^{m-1}\sum_{j=1}^{n-1} |I_{reg}(i, j) - I_{reg}(i, j-1)|$$

$$D_{Bver}(i, j) = \sum_{i=1}^{m-1}\sum_{j=0}^{n-1} |B_{ver}(i, j) - B_{ver}\ \ (i-1, j)|$$

$$D_{Bhor}(i, j) = \sum_{i=0}^{m-1}\sum_{j=1}^{n-1} |B_{hor}(i, j) - B_{hor}\ \ (i, j-1)| \quad (4)$$

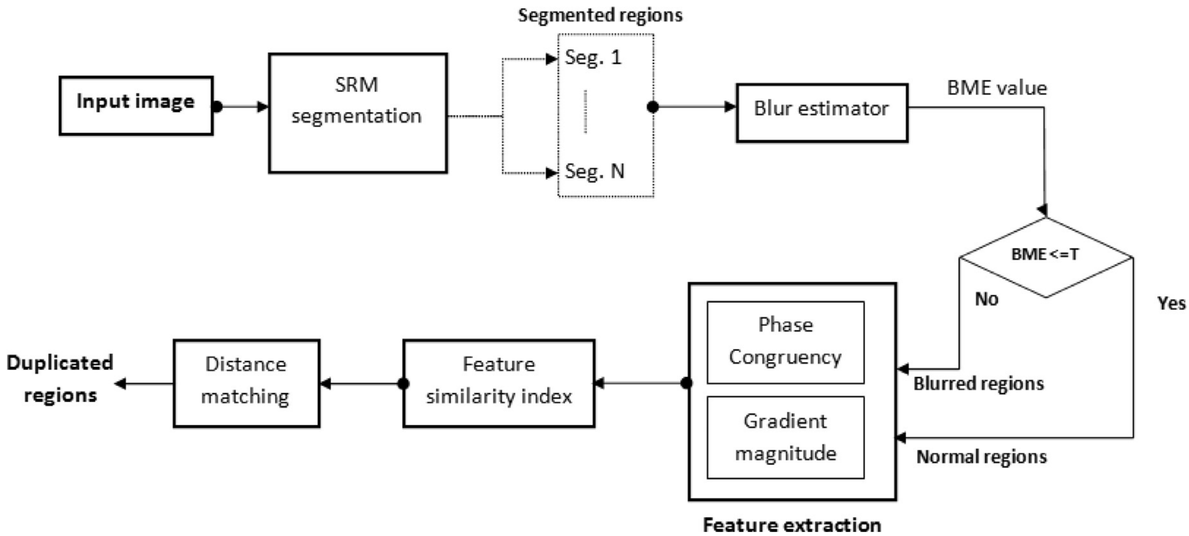

Fig. 2. Main steps of the proposed method.

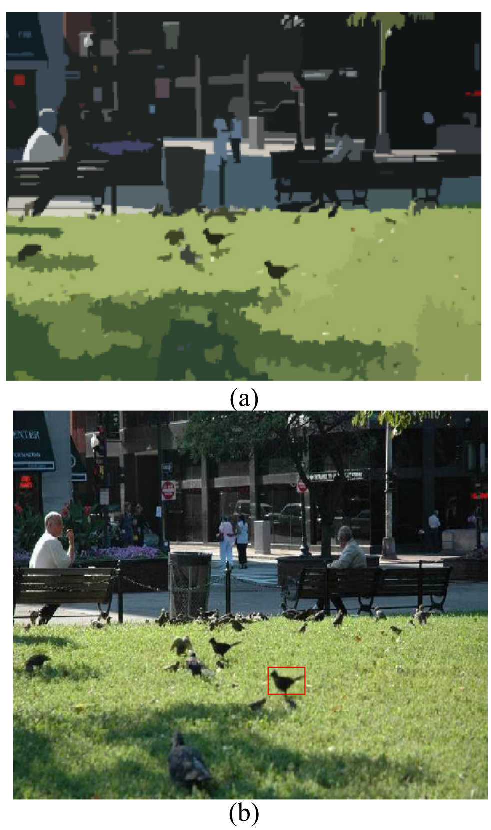

Fig. 3. Sample region of interest segmentation of the proposed method.

Step 3: The variation in the horizontal and vertical absolute difference images is evaluated by the Riemann integral as follows:

$$V_{hor} = \max(f(x), 0) = \begin{cases} f(x) = D_{Ihor} - D_{Bhor}, & f(x) \geq 0 \\ 0, & otherwise \end{cases} \quad (5)$$

Where V_{hor} and V_{ver} are the horizontal and vertical absolute difference images, respectively. They are computed in the same manner.

Step 4: The variations in the sum of the intensities of difference images D_{Iver}, D_{Ihor},D_{Bver}, and D_{Bhor} in a defined range [0–1] are normalized to estimate the vertical and horizontal blur measures as follows:

$$Blur_{Iver} = \frac{\Sigma\ D_{Iver} - \Sigma\ D_{V\,ver}}{\Sigma\ D_{Iver}},\ where\ D_{vver} = \Sigma\ D_{V\,ver}$$

$$Blur_{Ihor} = \frac{\Sigma\ D_{Ihor} - \Sigma\ D_{V\,hor}}{\Sigma\ D_{Ihor}},\ where\ D_{vhor} = \Sigma\ D_{V\,hor} \quad (6)$$

Step 5: The blur measure is selected as the maximum value among the vertical and horizontal measures.

$$\mathrm{BME} = \mathrm{Max}\,(Blur_{I_{ver}}, Blur_{I_{hor}}) \quad (7)$$

Where BME is in the range [0–1]; 0 indicates that the image is sharp and 1 suggests that it is blurred.

Sample results of the proposed degree of blur estimation are shown in Fig. 4 . The degree of blur is low for non-blurred images and high for blurred images.

A stem chart of the counts of each image BME is presented in Fig. 5. Normal regions generally correspond to the highest peak in the histogram. As a result, the detected blurred regions have BME values greater than that of non-blurred regions.

If the region BME value is greater than the value of BME at the highest peak, then the region is considered as blurred **ROI** else it is considered as non-blurred region ROI.

3.3. Forged blurred region identification

There exists blur in images due to object and camera movements, defocus. In this case, the step proposed in previous section may misclassify actual blurred region as forged region when BME values of the regions satisfy the threshold values. Therefore, we propose a new method for identifying actual forged blurred region from the non blurred region. However, in most cases, the normal blurred region may preserve structure of objects since it is affected by natural blur while forged blurred regions may lose shape due to copy and move process along with blurring procedure. This observation motivated us to propose the combination of Fourier coefficients based features and gradient features for studying the structure of the image regions.

For each blurred region, the proposed method obtain high frequency phase congruency (PCy) coefficients. The PCy for 2D images can be defined in terms of the Fourier transform of signal, f (x, y) at point (x, y) in the image as follows (Kovesi, 2003):

$$PCy(x, y) = \frac{\sum_n \sum_\theta\ W(x, y)\lfloor A_{n\theta}(x, y)\Delta\psi_{n\theta}(x, y) - T\rfloor}{\sum_n \sum_\theta\ A_{n\theta}(x, y) + \varepsilon} \quad (8)$$

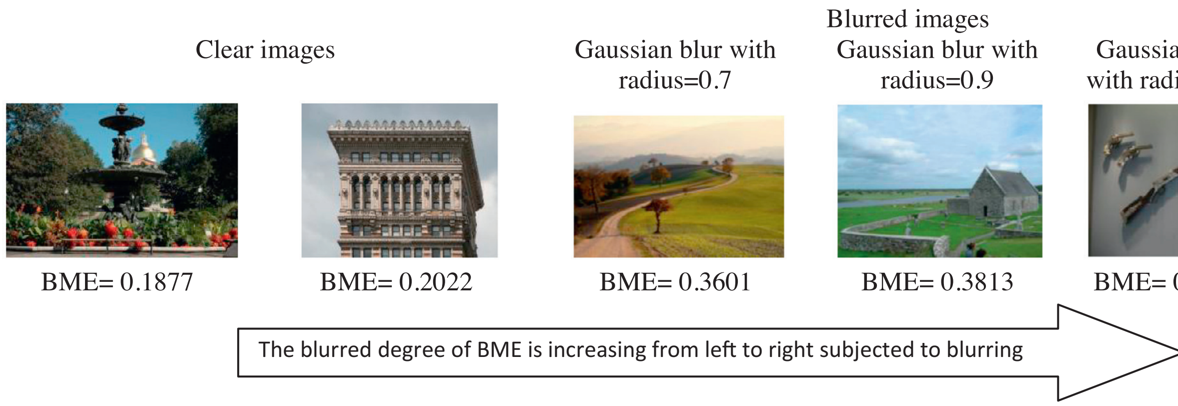

Fig. 4. Sample results for estimating degree of blur of the region of interests.

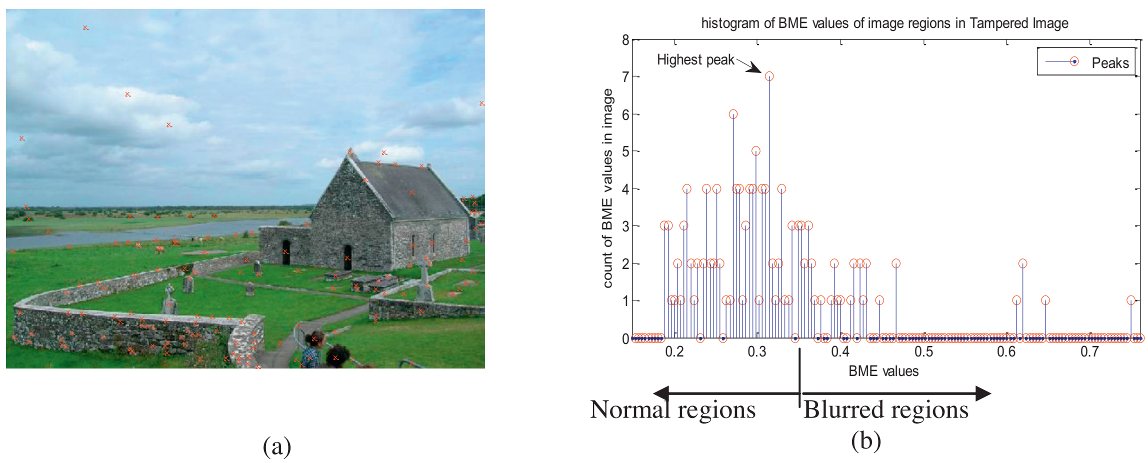

Fig. 5. Blurred and non-blurred region separation**:** **(a)** Centroids marked by red color of image regions given by segmentation method. **(b)** Histogram for BME values vs their frequencies to find dynamic threshold for separation.

where $W(x, y)$ is the weight function of the 2D log-Gabor filter at point $f(x, y)$. $\lfloor\,\rfloor$ is a floor function that equalizes the enclosed quantity to itself when its value is positive; otherwise, the value is zero. $A_{n\theta}(x, y)$ is the amplitude of the Fourier component at scale n and an orientation angle of filter θ can be defined as

$$A_{n\theta}(x,y) = \sqrt{e_{n\theta}(x,y)^2 + o_{n\theta}(x,y)^2} \tag{9}$$

where $e_{n\theta}(x, y), o_{n\theta}(x, y)$are the responses between image $f(x, y)$ and the 2D log-Gabor filter. They are expressed as follows:

$$[e_{n\theta}(x,y),\ o_{n\theta}(x,y)] = [f(x,y) * M^e_{n\theta}], \tag{10}$$

where * is the convolution operator. $M^e_{n\theta}$ *and* $M^O_{n\theta}$ are even and odd symmetric wavelets at scale $n=4$ and angle $\theta=6$, respectively. T is the estimated noise energy. $\varepsilon=0.0001$ is a small constant that prevents division by zero. $\Delta\psi_{n\theta}(x, y)$ is the sensitive measure of phase deviation that is written as follows:

$$\Delta\psi_{n\theta}(x,y) = \cos(\psi_{n\theta}(x,y) - \bar{\psi}_{n\theta}(x,y)) - \left|\sin(\psi_{n\theta}(x,y) - \bar{\psi}_{n\theta}(x,y))\right| \tag{11}$$

The PCy coefficients are real numbers in the range [0–1]; 0 corresponds to low-frequency components, whereas 1 denotes the highly informative features in the image. The result of PCy is shown in Fig. 6 where it can be seen that Phase congruency highlight the significant information especially edges in the image which results in enhanced image by suppressing blur information and background information. Furthermore, PCy features are robust to blur operation as shown in Fig. 6, where there is a similarity between histograms of duplicated regions in PCy map image.

For such enhanced blurred ROI**,** the proposed method extract three moments, namely, mean (μ), variance (υ), and contrast (c) and it is considered as feature vector, $F=(\mu, \upsilon, c)$. This vector is used for matching to identify forged blurred region.

In the same way, the proposed method extracts gradient features for the enhanced blurred ROI as follows:

The directional gradients along x and y axis of image I are defined as:

$$\nabla I_x = \frac{L(x+1,y) - I(x-1,y)}{2},\ \nabla I_y = \frac{L(x,y+1) - L(x,y-1)}{2}.$$

Where L(x, y) is a derivative of image I with Gaussian kernel. Gradient magnitude is estimated as the square root of the sum of image directional gradients. That is,

$$GM = \sqrt{\nabla {I_x}^2 + \nabla {I_y}^2}. \tag{12}$$

GM features are extracted as secondary features from each image region in the forged image and are then combined with PCy features to estimate a similarity index measure of the image region. The three moments features and gradient features are combined for finding the similarity and dissimilarity to classify whether the given region is forged blurred region or non blurred region using Euclidean distance measure. The regions which have high degree of similarity are classified as forged blurred regions.

The Euclidean distance D (R_x, R_y) determines the distance between regions R_x and R_y. FX and FY are the corresponding features vectors of N dimensions of the matched regions with edge points.

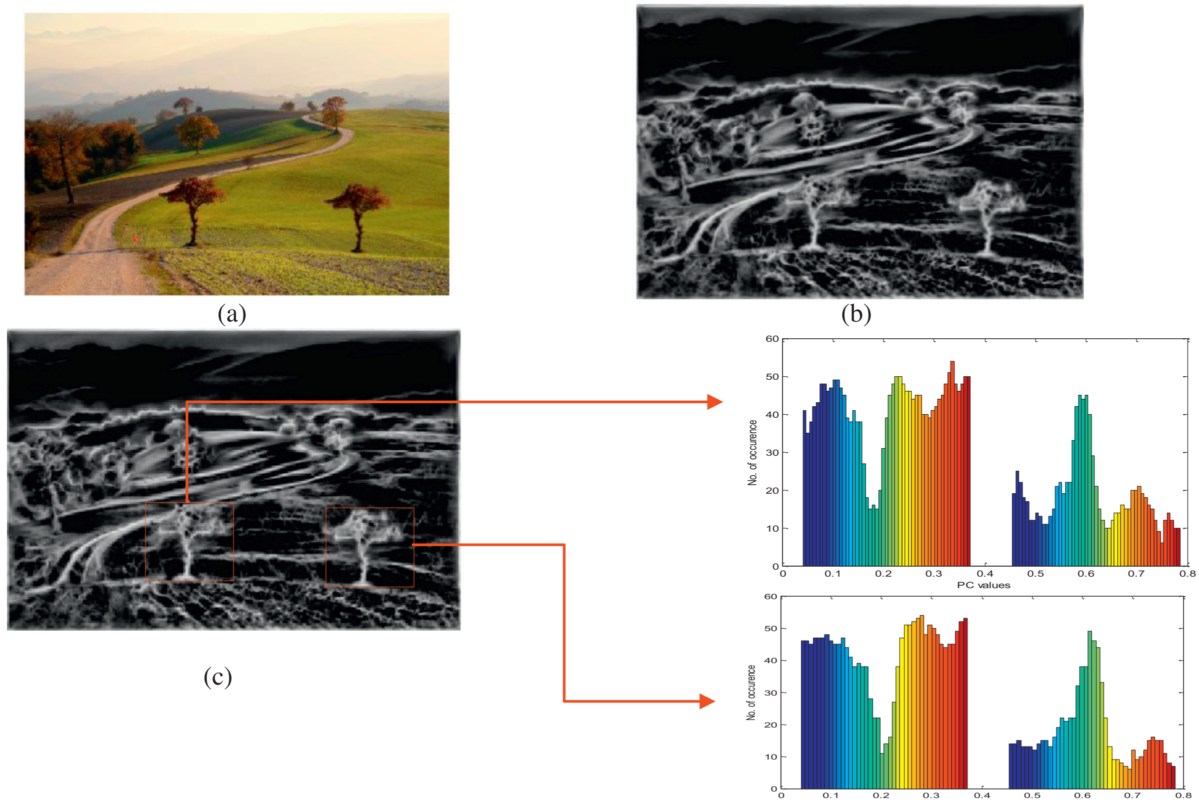

Fig. 6. Illustrating enhanced image by Fourier coefficients. (a) Image "tree" has blurred copy–move forgery with Gaussian blur (radius = 0.8). (b) PCy map of (a) to obtain a significant mapping of internal structure of foreground objects such as edges. (c) selected ROIs in PC map including normal tree in the left side and blurred cloned tree in the right side and the histograms of selected ROIs in PC map to show robustness to blur.

The Euclidean distance is expressed as follows:

$$D(R_x, R_y) = \sqrt{\sum_{i=1}^{N} (FX_i - FY_i)^2} \tag{13}$$

Finally, the duplicate regions are located along with their centroids. The blurred region is highlighted by a circle to visualize the forged region in the image.

4. Experimental results

In order to evaluate the proposed method, we consider two standard datasets, namely MICC-F220 data which contains 110 forged images and 110 original images (Amerini, Ballan, Caldelli, Del Bimbo, & Serra, 2011) and one more, Image manipulation dataset which contains 48 true-color images (Christlein et al., 2012). These datasets provide small duplicated regions with repetitive patterns which are required to create forgery content using postprocessing operation such as blurring, additive noise. In this study, we use Gaussian blur kernel to blur the repeated pattern regions. The parameters for similarity score is set experimentally to $T = 0.91$. To measure the performance of the proposed method, we use true positive rate (T_{PR}), and false positive rate (F_{PR}).

4.1. Evaluating segmentation step

The segmentation step of the proposed method is vital for achieving better results. Therefore, to analyze the contribution of segmentation steps, we compare the proposed segmentation results with well-known state of the art existing segmentation methods namely: the method in Shi & Malik, (2000), the method in Chen, Chen, & Chien, (2008) and proposed segmentation as shown in Fig. 7. Ncut algorithm treats with a Graph partitioning problem. A normalized cut condition based on eigenvectors is employed for segmenting the graph.

Chen et al., (2008) proposed a color image segmentation based HSV features with K-means clustering. The weakness of their method is that, it could lead to improper segmentation results when the image has too small regions. Fig. 7 shows that the proposed segmentation works well compared to the existing methods because the proposed method considers statistical analysis as well as color texture for segmentation. The reason for the poor results of the existing methods is that the features used in their methods are sensitive to background and blur information.

4.2. Evaluating the proposed forged blur detection

Sample qualitative results of the proposed method for detecting forged blurred region are shown in Fig. 8 where it can be seen that the proposed method detects well for the different background images. In order to test robustness of the proposed method, we conduct experiments by varying the degree of blur radii parameters (0.3, 0.5, 0.9, 2.0, and 3.0).

Quantitative results of the proposed method on both standard datasets are reported in Table 1. As shown in Table 1, the proposed method achieves good detection results which are more than 90% for both images datasets. However, still the proposed method fails for few images when segmentation fails to segment regions correctly.

Based on the analysis of blurred duplicate regions in the images mentioned in Table 2, we reveal that the blur metric measure increases for the blurred region as the blur radius increases.

The proposed method has been tested also under JPEGcompression, and white Gaussian noise attacks, as shown in Fig. 9.

Fig. 7. Sample qualitative results of the proposed and existing segmentation methods.

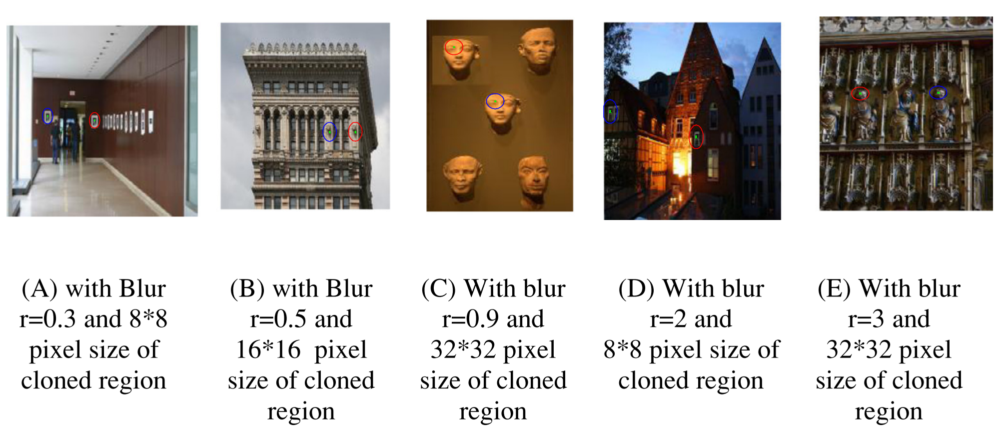

Fig. 8. Detection results of the forged images A–E subject to blurring at various blur radii on two image datasets.

Table 1
Detection results of blurred copy–move forgery.

Image database	Number of mage	Average detection rate	
		T_{PR}	F_{PR}
MICC-F220 (Amerini et al., 2011).	110	0.963	0.063
Image data manipulation (Christlein et al., 2012).	48	0.958	0.062

Table 2
Robustness of the proposed method to blurring manipulation on sample images.

Forged images	Blur radius	BME of duplicated regions		Similarity score
		$BME_{\text{before blur}}$	$BME_{\text{after blur}}$	
A	0.3	0.2301	0.2915	0.9552
B	0.5	0.2729	0.2735	0.9685
C	0.9	0.5554	0.5914	0.9648
D	2	0.2179	0.2325	0.9405
E	3	0.3569	0.4166	0.9111

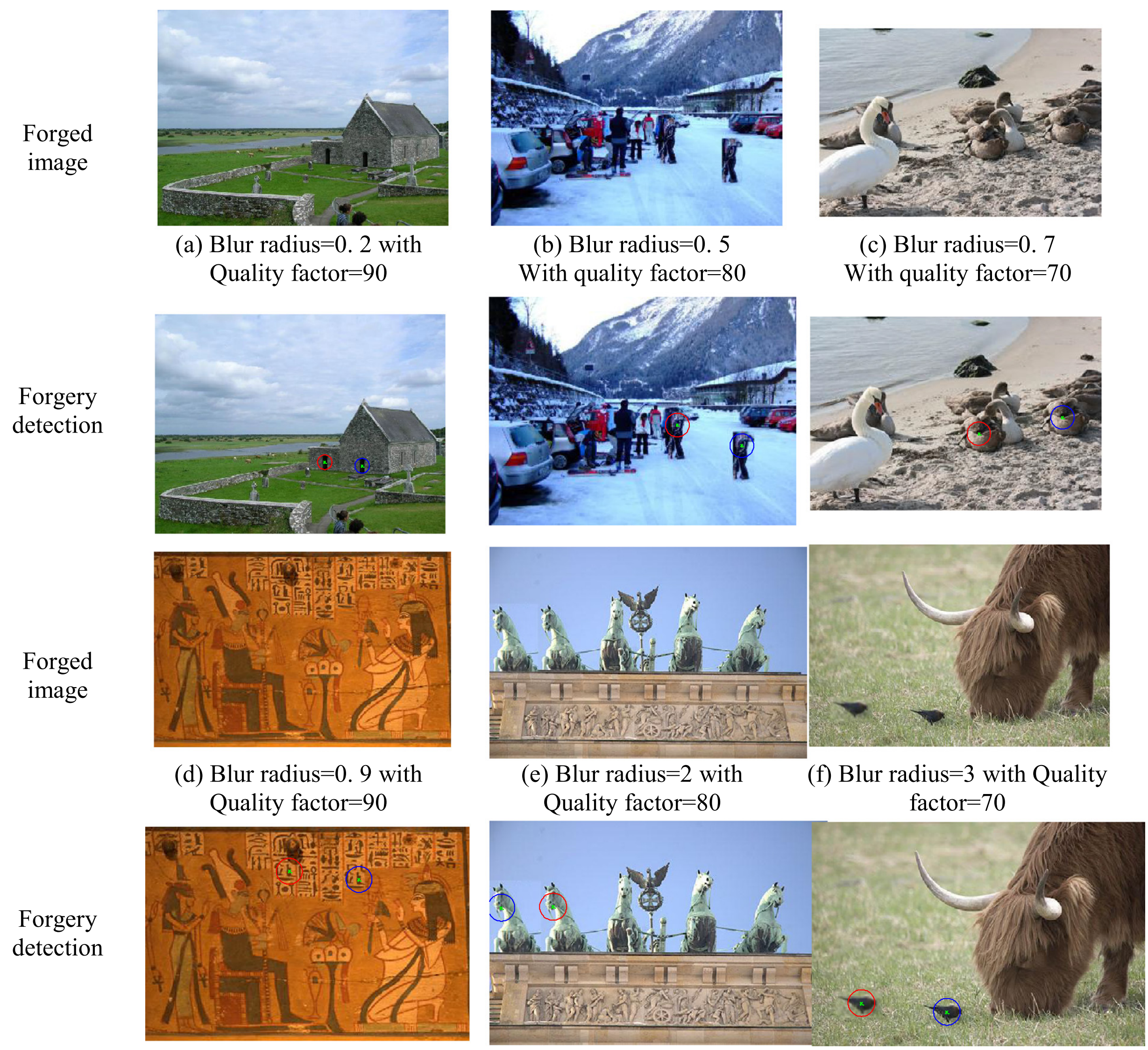

Fig. 9. Detection results of tampered images (a)–(f) under various Gaussian blurring radii, and with various quality factors.

As shown in Fig. 9, the proposed method can successfully detect the forgeries under under different quality compression factors and noise levels for both the datasets.

The quantitative results for JPEGcompression, and white Gaussian noise attacks are reported in Tables 3, and 4 respectivly.

It can be observed that the proposed method achieves good result for both image datasets on both the experiments. This shows that the proposed method not only detects forged blurred region well but also robust to quality of the image and noise.

Table 3
The average detection rate of blurred copy move forgery for JPEG compression. Each data point corresponds to an average of 100 images from two image database: MICC-F220 and Image data manipulation.

Quality factors		90	80	70	60	50
MICC-F220	T_{PR}	0.96	0.90	0.92	0.84	0.90
	F_{PR}	0.06	0.08	0.08	0.10	0.10
Image data manipulation	T_{PR}	0.95	0.91	0.92	0.88	0.90
	F_{PR}	0.05	0.07	0.07	0.19	0.19

(a) Original image with low contrast. (b) Results of Segmentation

Fig. 10. The detection results of SRM segmentation method.

Table 4
The average detection rate of blurred copy move forgery under AWGN on image datasets.

SNR(dB)		35	30	25	20	15
MICC-F220	T_{PR}	0.92	0.95	0.95	0.96	0.97
	F_{PR}	0.10	0.10	0.10	0.06	0.06
Image data manipulation	T_{PR}	0.93	0.93	0.94	0.95	0.97
	F_{PR}	0.09	0.10	0.19	0.06	0.07

4.3. Comparative study

To show the effectiveness of the proposed method, we compare the proposed method results with well-known state of the art methods. The methods considered for comparative study are: the method which uses SIFT keypoints as in Amerini et al., (2011); the method which uses transform-invariant features as in Kakar & Sudha, (2012); the method which uses SURF with hierarchical agglomerative clustering as in Mishra, Mishra, Sharma, & Patel, (2013), and another two methods (Mahdian & Saic, 2007; Wang et al., 2013) which consider blur region duplication in forged images.

The quantitative results of the proposed and existing methods are reported in Table 5 on both the datasets. Table 5 shows that the proposed method is best at false positive rate compared to all existing methods while it is best at detection rate compared to all existing methods except (Amerini et al., 2011). However, Amerini (Amerini et al., 2011) requires high dimension to achieve better results compared to the proposed method. Therefore, we can conclude that the proposed method is accurate and efficient to use in real time applications.

4.4. Limitation

It is noticed from the proposed method that blur information is important to identify the forged region in the image. It is obvious that when the image contains high degree of blur, the performance of the proposed method will degrade significantly. According to experimentation, it is true that the proposed segmentation step work well when the foreground of regions have high contrast compared to its background. However, if the image contains regions which camouflage with the background. As shown in Fig. 10 where one can see the bird on buffalo's head overlap with the buffalo. Even our vision system fails to identify the bird on buffalo. In this case, the proposed segmentation fails to detect this region due to the low contrast transition between copied region and its background. This shows that there is a scope for improvement and future work. We consider these issues in near future by exploring context features for identifying forged regions in these situations.

5. Conclusion and future work

We have proposed a novel method for identifying tampered blurred regions in the image. First, the proposed method introduces a new color texture features for segmenting region of interest irrespective of degree of blur and distortion effect. For each segmented region of interest, the proposed method estimates degree of blur by exploring blur metrics which involves study of variation of neighbor pixel information. This results in separating blurred regions irrespective of normal blurred regions and forged blurred regions. The blurred regions are validated by the new combination of Fourier coefficients based features and gradient features to identify the forged blurred regions based on similarity y score between the regions. The similarity between the blurred regions are estimated using Euclidean distance measure. Experimental results on standard datasets show that the proposed method is capable of detecting forged region under different situations. The robustness of the proposed method is tested by conducting experiments on different degree of blurriness, quality image and level of noise. The effectiveness of the proposed method is tested by comparing with the existing methods. The results show that the proposed method outperforms the existing methods in terms of T_{PR} and F_{PR}. However, the current limitation of the proposed method is that sometimes, segmentation method fails to segment region of interest properly when the image contains too complex background and too low resolution. Therefore, our next target is to investigate new segmentation method to achieve still better results in complex situations.

Table 5
Comparisons with other methods for region duplication forgery detection on MICC-F220 and image data manipulation dataset.

Methods	MICC-F220		Image data manipulation		Feature dimension
	T_{PR}	F_{PR}	T_{PR}	F_{PR}	
(Amerini et al., 2011)	100	8	NA	NA	128
(Kakar & Sudha, 2012)	90	3	NA	NA	NA
(Mishra et al., 2013)	73.6	3.64	NA	NA	64
(Mahdian & Saic, 2007)	NA	NA	88.89	NA	24
(T. Wang et al., 2013)	NA	NA	40	70	4
The proposed method	**96.5**	**2.86**	**97**	**2.6**	**3**

Conflict of interest

The authors declare that there is no conflict of interests regarding the publication of this article.

Author contributions

All authors jointly worked on deriving the results and approved the final manuscript**.**

Acknowledgment

The authors would like to thank the reviewers for their comments and suggestions for improving the paper. This research is funded by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (FRGS), project No.: FP073-2015A.

References

Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International, 231*(1), 284–295.

Almohammad, A., Ghinea, G., & Hierons, R. M. (2009). JPEG steganography: A performance evaluation of quantization tables. *Paper presented at the 2009 international conference on advanced information networking and applications*.

Almohammad, A., Hierons, R. M., & Ghinea, G. (2008). High capacity steganographic method based upon JPEG. *Paper presented at the availability, reliability and security, 2008. ARES 08. third international conference on*.

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

Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital Investigation, 10*(3), 226–245 *September 2013*.

Chen, T.-W., Chen, Y.-L., & Chien, S.-Y. (2008). Fast image segmentation based on K-Means clustering with histograms in HSV color space. In *Paper presented at the multimedia signal processing, 2008 IEEE 10th Workshop on* (pp. 322–325).

Christlein, V., Riess, C., Jordan, J., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches 1-26. In *IEEE transactions on information forensics and security* (pp. 1–26).

Crete, F., Dolmiere, T., Ladret, P., & Nicolas, M. (2007). The blur effect: Perception and estimation with a new no-reference perceptual blur metric. *Paper presented at the Electronic Imaging 2007*.

Guo, J.-M., Liu, Y.-F., & Wu, Z.-J. (2013). Duplication forgery detection using improved DAISY descriptor. *Expert Systems with Applications, 40*(2), 707–714.

Huang, D.-Y., Lin, T.-W., Hu, W.-C., & Chou, C.-H. (2014). Boosting Scheme for Detecting Region Duplication Forgery in Digital Images. In *Genetic and evolutionary computing, Volume 238 of the series advances in intelligent systems and computin* (pp. 125–133). Springer.

Huo, Y., He, H., & Chen, F. (2013). A semi-fragile image watermarking algorithm with two-stage detection. *Multimedia Tools and Applications*, 1–27. doi:10.1007/s11042-012-1317-4.

Kakar, P., & Sudha, N. (2012). Exposing postprocessed copy–paste forgeries through transform-invariant features. *Information Forensics and Security, IEEE Transactions on, 7*(3), 1018–1028.

Kang, X., Li, Y., Qu, Z., & Huang, J. (2012). Enhancing source camera identification performance with a camera reference phase sensor pattern noise. *Information Forensics and Security, IEEE Transactions on, 7*(2), 393–402.

Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., & Pevný, T. (2013). Moving steganography and steganalysis from the laboratory into the real world. In *Paper presented at the proceedings of the first ACM workshop on Information hiding and multimedia security* (pp. 45–58). ACM New York, NY, USA.

Kessler, G. (2004). An overview of steganography for the computer forensics examiner. *An edited version, issue of Forensic Science Communications, 6*(3), 1–27.

Kovesi, P. (2003). Phase congruency detects corners and edges. *Paper presented at the The australian pattern recognition society conference: DICTA 2003*.

Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*(2), 142–172.

Li, C.-T. (2010). Source camera identification using enhanced sensor pattern noise. *Information Forensics and Security, IEEE Transactions on, 5*(2), 280–287.

Lin, H.-J., Wang, C.-W., & Kao, Y.-T. (2009). Fast copy-move forgery detection. *WSEAS Transactions on Signal Processing, 5*(5), 188–197.

Liu, G., Wang, J., Lian, S., & Dai, Y. (2013). Detect image splicing with artificial blurred boundary. *Mathematical and Computer Modelling, 57*(11), 2647–2659.

Mahdian, B., & Saic, S. (2007). Detection of copy–move forgery using a method based on blur moment invariants. *Forensic Science International, 171*(2), 180–189.

Mishra, P., Mishra, N., Sharma, S., & Patel, R. (2013). Region duplication forgery detection technique based on SURF and HAC. *The Scientific World Journal, 2013*.

Nock, R., & Nielsen, F. (2004). Statistical region merging. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 26*(11), 1452–1458.

Hayati, P., P. , V., & Chang, E. (2007). A survey of steganographic and steganalytic tools for the digital forensic investigator. *Paper presented at the the workshop of information hiding and digital watermarking, Moncton, New Brunswick, Canada*.

Piva, A. (2013). An overview on image forensics. *ISRN Signal Processing, Volume, 2013*(2013), 1–22.

Potdar, V. M., Khan, M. A., Chang, E., Ulieru, M., & Worthington, P. R. (2005). e–Forensics steganography system for secret information retrieval. *Advanced Engineering Informatics, 19*(3), 235–241.

Rao, C. S., & Babu, S. T. (2016). Image authentication using local binary pattern on the low frequency components *microelectronics*. *Electromagnetics and Telecommunications (Vol. Volume 372 of the series Lecture Notes in Electrical Engineering, pp 529-537., pp. pp 529-537). India, 372*, 529–537 of the series Lecture Notes in Electrical Engineering.

Shan, Q., Jia, J., & Agarwala, A. (2008). High-quality motion deblurring from a single image. *Paper presented at the ACM Transactions on Graphics (TOG)*.

Shao, H., Yu, T., Xu, M., & Cui, W. (2012). Image region duplication detection based on circular window expansion and phase correlation. *Forensic science international, 222*(1), 71–82.

Sheng, G., Gao, T., Cao, Y., Gao, L., & Fan, L. (2012). Robust algorithm for detection of copy-move forgery in digital images based on ridgelet transform. In *Artificial intelligence and computational intelligence* (pp. 317–323). Springer.

Shi, J., & Malik, J. (2000). Normalized cuts and image segmentation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 22*(8), 888–905.

Singh, C., & Ranade, S. K. (2013). Geometrically invariant and high capacity image watermarking scheme using accurate radial transform. *Optics & Laser Technology, 54*, 176–184.

Wang, J., Liu, G., Xu, B., Li, H., Dai, Y., & Wang, Z. (2010). Image forgery forensics based on manual blurred edge detection. *Paper presented at the 2010 international conference on multimedia information networking and security*.

Wang, T., Tang, J., & Luo, B. (2013). Blind detection of region duplication forgery by merging blur and affine moment invariants. *Paper presented at the Image and Graphics (ICIG), 2013 seventh international conference on*.

Zhang, W., Wu, Q., Wang, G., You, X., & Wang, Y. (2010). Image matching using enclosed region detector. *Journal of Visual Communication and Image Representation, 21*(4), 271–282.

Zheng, J., & Liu, M. (2009). A digital forgery image detection algorithm based on wavelet homomorphic filtering *Digital Watermarking* (pp. 152–160): Springer.

Zhou, L., Wang, D., Guo, Y., & Zhang, J. (2007). Blur detection of digital forgery using mathematical morphology. In *Agent and multi-agent systems: Technologies and applications* (pp. 990–998). Springer.