Forensic Imaging 22 (2020) 200385

Contents lists available at ScienceDirect

Forensic Imaging

journal homepage: www.sciencedirect.com/journal/forensic-imaging

Investigation of image forgery based on multiscale retinex under illumination variations

Diaa M. Uliyan*, Mohammad T. Alshammari

Department of Information and Computer Science, College of Computer Science and Engineering, University of Ha'il, Ha'il, 81481, Saudi Arabia

ARTICLE INFO

Keywords:
image forensics
region duplication forgery
illumination invariant features
image segmentation

ABSTRACT

The number of forged images is currently expanding vastly over the Internet. Therefore, image authenticity represents a globally challenging issue that must be addressed. Emerging tools for image editing have been developed to manipulate and enhance digital images; however, forgers can exploit these tools to achieve their destructive purposes. Forgers often use a common method of image forgery called region duplication forgery. In this method, the copied region in the fake image can appear identical to the original region of the image. This paper aims to target this issue by developing an algorithm that can detect suspected images through localizing small duplicated regions. These regions can be described by multiscale features, which are invariant with illumination variations. The proposed method begins with segmenting suspected images using an adaptive statistical region merging. The goal of the segmentation method is to discover small regions. The method then targets the small regions based on color correction to represent their illumination features. Experiments are also conducted to validate the proposed method on two image datasets, Media Integration and Communication Center (MICC) and Image Data Manipulation, yielding positive results. A comparative study of the most recent methods is carried out.

Introduction

Advancement of photo editing technologies can be exploited by image forgers. In addition, the widespread dissemination of fake images via social media and news can make a better ground for deliberate deception or a harmful hoax. Counterfeiting images can also be done easily, even by novices, which is a challenging issue that must be explored. To address this issue, image authentication is needed to verify and detect image changes. There are two main image authentication approaches—active authentication [1] and passive authentication [2]. In the active authentication approach, watermarking and steganography can be used by embedding a piece of digital information into an original image. The digital information is employed to examine whether an image has been forged without revealing the locations of the forged regions. However, the active approach results in some distortions, which affect the quality of the original image. In contrast, passive approaches have been developed to investigate the authenticity of duplicated regions in a forged image without demanding any explicit embedment of information or content. The main idea of the passive authentication approach is to explore pixel irregularities and correlations in the image [3]. Different methods can be used for passive authentication approach [4] and these are categorized into different schemes, such as pixel correlation, format analysis, source camera identification, physics-based methods, and geometry analysis. The pixel correlation method exploits the content-based image features and their correlation for the detection of forgery. It examines the amount of consistency at the pixel level in the forged image [5]. The methods of format analysis leverage the statistical correlations introduced by a specific lossy compression technique [6]. Source camera identification utilizes artifacts introduced by the camera lens, sensor, and so on [7]. Physics-based methods exploit illumination inconsistencies introduced by light direction and lightning environments that serve as evidence of an image forgery [8]. Geometry analysis methods make measurements of objects in the world and their positions relative to the camera [9].

Many images have been forged via three common forgery techniques, which are as follows: splicing [10, 11], retouching [12], and region duplication [5, 13]. Image splicing creates a new image type of forgery by composing two different images [14]. Retouching aims at filtering out the image by fluctuating some of its features while keeping the original content [12]. Region duplication uses a tool for selecting, copying, and moving an object or region within an image to hide some content or duplicate regions. Specifically, small regions can be targeted

Diaa Uliyan is an Assistant Professor in University of Ha'il, College of Computer Science and Engineering

* Corresponding author:

E-mail addresses: d.uliyan@uoh.edu.sa (D.M. Uliyan), md.alshammari@uoh.edu.sa (M.T. Alshammari).

https://doi.org/10.1016/j.fri.2020.200385

Received 21 January 2020; Received in revised form 5 May 2020; Accepted 25 May 2020

Available online 28 May 2020

for better forgery. Forgers usually modify the duplicated regions via geometric operations and post-processing operations to merge the duplicated region with its surrounding area [15]. In this paper, we focus on one type of forgery called region duplication, as it is one of the most common forgery detection techniques [16].

Considering the ease of fraud perpetration via photo editing applications, it is necessary to develop forgery detection algorithms that validate the integrity of an image through a single scheme or hybrid schemes where multiple approaches are run in combination. A popular scheme is region duplication detection; this can localize clone patches in the image [17]. While these cloned regions have the same pixel data in the source image, forgers can apply illumination changes to the cloned regions. The illumination creates irregularities between the original regions and fake regions to challenge the identification of the forgery. There is a high demand for finding robust detection features against illumination changes. In this paper, we propose an illumination-invariant scheme to detect copy–move forgery even for considerably small duplicated regions to improve detection accuracy.

Related Work

Different region duplication detection approaches have been developed [18]. The common framework of detection methods involves five key steps, which are as follows: image preprocessing, feature extraction, descriptor building and saving into a feature vector, matching, and visualization [19]. The most common forgery detection schemes consider two types of attacks to localize forged regions (post-processing operations and geometric transformations), as introduced in Fig. 1. On the one hand, post-processing operations include blurring [15] by targeting edge regions [20-22] or the whole forged region [23] and illumination changes [24-26]. Forgers utilize post-processing operations to conduct undetectable tampering and hide artifacts. On the other hand, geometric transformations involve scaling [27-29] and rotation [30]. A robust detection method needs to adapt a statistical descriptor to combat scaling or rotation attacks [31, 32].

The process of extracting features is a core element of forgery detection methods. It highlights appropriate pixel data to characterize the region of interest in an image. Selecting regions of interest in the image can decrease time complexity in the matching step. The region of interest in forgery detection methods is classified into three main classes [33], which are as follows: block-based methods [34, 35], segmentation-based methods [35, 36], and key points–based methods [29, 36, 37].

In the block-based method, the image is fragmented into either square or circle blocks [38]. For each block, features are extracted and saved in a feature vector. Some methods transform the image blocks into the frequency domain [17, 35, 39], wavelet domain [34, 40], color-based information [41, 42], statistical texture information [44], or statistical moments [43]. The main advantage of the block-based method is the suitability of examining similar textured regions with minimal details. Forgers usually employ texture regions to hide information in an image; they employ geometric features, such as scaling and rotation [44, 45].

Image segmentation can be used as a preprocessing step in the forgery detection method. The image is split into multiple regions based on the characteristics of their pixels. These pixels represent such objects or homogeneous regions. Noise estimation can then be applied to segmented regions to find matched features from the image [46, 47].

In the key points–based method, local interest points are detected from the image. These key points represent the internal structure of the image. This internal structure may have some primitives, such as corners or edges. The group of primitives can be connected to shape a non-uniform region. The key points detection method aims at detecting forged non-uniform regions by various techniques, such as scale-invariant features transform (SIFT) [28, 29, 48], speeded up robust feature (SURF) [49, 50], Harris corners [30, 51], and efficient dense descriptor applied to wide baseline stereo (DAISY) [43]. As mentioned in Christlein et al. [13], the main advantage of key points is the robustness to some geometric operations, such as scaling and rotation operations. The main drawback is the weak detection rate of non-uniform regions against illumination changes [52]. Moreover, detection accuracy is still low when forged regions have a uniform texture. To address this issue, a forgery detection method should extract robust features via fluctuating the intensity levels of all pixels. For instance, Davarzani et al. [25] divided the image into overlapping blocks, which are filtered by a wiener filter to preserve the edges and high-frequency contents in an image. Then, centric symmetric local binary patterns are extracted from each block to use different neighborhoods of pixels 8, 12, or 16 with different radius sizes. Feature vectors are saved and sorted based on lexicographical sorting. False-positive rates of the detection method are then eliminated by a random sample consensus (RANSAC), and forged duplicate regions are visualized. Fan et al. [24] were able to detect forged regions where an image is divided into blocks. For each block, they extracted features based on gradient orientation and local intensity differences. Gradient distributions were pooled within such order blocks. The ordering information was then encoded and saved into a descriptor via the pooling strategy to represent it as a two-dimensional histogram. In Muhammad et al. [53], the image was converted into YC_bC_r chrominance space. Steerable pyramid transform (SPT) was applied on the chroma components to build multiscale bands. For each band, a local binary pattern (LBP) histogram was computed as features. A support vector machine (SVM) was applied to classify tampered regions.

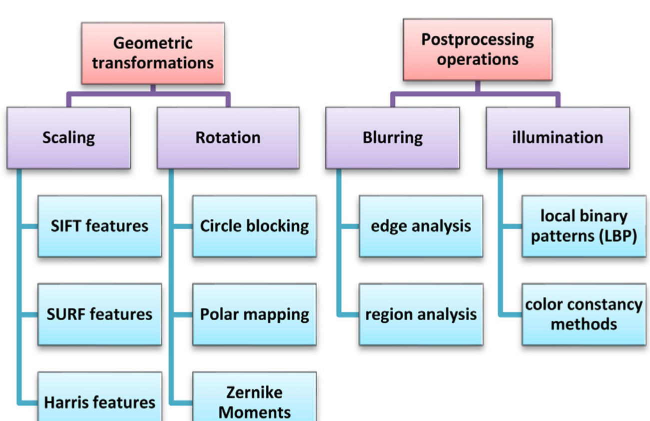


Fig. 1. Forgery detection methods based on geometric and post-processing operations.

The Proposed Method

To achieve good performance in detecting uniform regions against illumination changes, we propose a novel method for revealing post-processed copy–move forgery. The method utilizes statistical region merging (SRM) segmentation method to segment an image. Then, a multiscale retinex (MSR) with color distribution is employed to improve the color of regions. A multiscale integral center symmetric census transform (MI-CSCT) is then applied. MI-CSCT is a normalization technique aimed at rendering regions in such a way that a post-processed image is free of illumination variations. The main contribution of this work is that the SRM algorithm is adapted to partition the image into small regions, where the least frequent regions can be identified. Then, the proposed method perceives objects in an invariant manner despite variations in illumination. Finally, matching feature constraints are utilized to improve the detection rate of the proposed method via adaptive fuzzy C means (FCM) clustering technique. The main aim of the proposed method is to expose region duplication forgery against

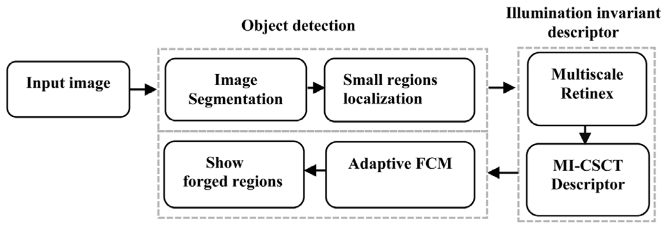


Fig. 2. illustrates the main steps of the proposed method.

illumination changes. Figure 2 illustrates the flowchart of the proposed method.

Image segmentation

The main purpose of the segmentation technique is to highlight the regions of a specific image. This technique selects similar regions that have the same color pattern. It is vital to detect the forged duplicated regions by the segmentation process due to their similarity on the color palette. We adapt a statistical region merging (SRM) method with our proposed method to detect duplicated regions. SRM consists of two main components—the merging predicate and testing order. The merging predicate detects objects based on color differences of the color channel *(Red, Green, Blue)*; it then applies the region merging method to create objects and assign the segment number for each object. Segment numbers are saved into the mapped image. In contrast, the testing order is motivated by the least frequent method, and it reads the assigned segment numbers in the mapped image row wise and column wise. The least frequent method is employed to select only small segmented regions.

Merging predicate

The SRM method is a bottom-up process that integrates image pixels into larger regions based on the predicate criteria. The merging predicate of an image has two common criteria, which are as follows: (1) inside any region, statistical pixels have the same mathematical expectation values for any given channel; and (2) the expectation values of adjacent regions are different for at least one color channel. Hence, a suitable merging predicate is applied according to these two criteria, as described by Nock and Nielsen [54]. The input image I contains $|I|$ pixels. Each pixel contains *RGB* values that represent a color channel $a \in \{R, G, B\}$. Each of the three values belongs to the set $S = \{1, 2, \ldots, g\}$. In the 8-bit image I, $g = 256$. This value represents the number of expected different colors. Each color channel is replaced by a new set of exactly Q independent random variables that derive the positive values in $[0, g/Q]$. The Q parameter can quantify the statistical complexity of a mapped image. High Q values result in a fine segmentation; thus, additional regions are generated by $b(R)$, which is a predicate function for region R. It is defined as follows:

$$b(R) = g\sqrt{\frac{1}{2Q|R|}\cdot In\left(\frac{|S_{|R|}|}{\delta}\right)}, \tag{1}$$

Where $In(\,)$ is the natural logarithm of each element in S and δ is a possible error with a small value; it is defined as $\delta = \frac{1}{(6\,|\,I\,|^{2})}.\, S_{|R|}$ is defined as set of areas with $|R|$ pixels. Q is in the limit *[1–256]*. Each segmented region is considered a closed region called an object. These regions have the following characteristics [55]: (1) homogeneity of the object is a common texture feature presented in *RGB* color channels; (2) the separability of pixels is defined as the pixel values of neighboring regions, which are dissimilar for at least one channel.

We assume that R and R' are two adjacent regions with color averages $|\bar{R}_a|$ and $|\bar{R}'_a|$ for channel a. To complete the merging, the merging predicate can be introduced in [54] as follows:

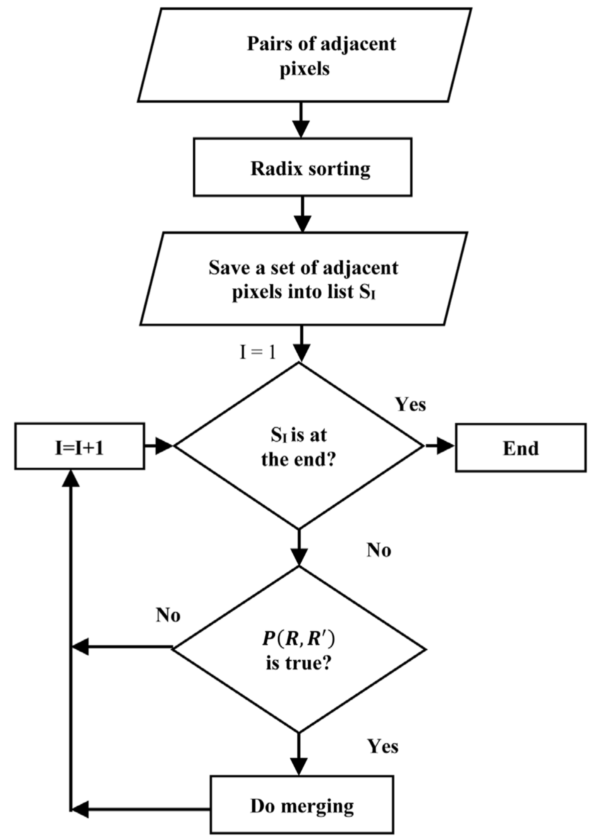


Fig. 3. Flowchart of the segmentation method based on SRM.

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

If $P(R,\ R') =$ True, then the two regions R and R' can be merged to shape larger regions in the image.

Testing order

The testing order technique considers only the adjacent pixels when the merging predicate begins to merge each pixel with its four neighbor pixels in the same region. It initially stores these pixels in pairs and sorts them later. The merging predicate completes the testing order and simply merges them, as presented in Fig. 3.

In the figure, the input image I has the number of testing orders $=$ $N < 2|I|$. The set of possible pairs of adjacent pixels is saved into S_I, which is sorted using the radix algorithm defined in [54], as follows:

$$d(p, p') = \max_{a \in \{R,G,B\}} |p'_a - p_a| \ , \tag{3}$$

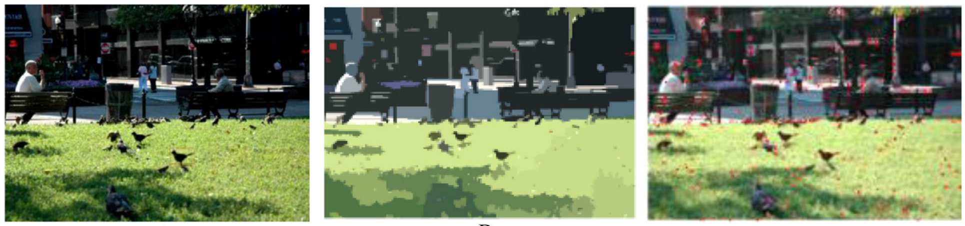
where $p_a,\ p'_a \in S_I$ are pairs of adjacent pixels in channel a.

When the SRM segmentation steps are completed, the mapped image I_M is created such that all candidate regions in the image have various sizes. To label only small regions, we search the mapped image in a row-wise and column-wise manner. This is defined by the following equation:

$$B = [unique(\bmod e_{row}(I_M(row,\ cols)) \cup unique(\bmod e_{cols}(I_M(row,\ cols))], \tag{4}$$

where B is the set of all possible more significant objects found in the mapped image horizontally and vertically. The *mode*(*image I*) function in MATLAB contributes to SRM by finding the most frequently occurring pixels in I_M. Small objects are then saved into set C, where C calculates the difference of two sets as $C = I_M - B$.

All detected small objects in the image should have a centroid. Each



A B C

Fig. 4. SRM method with small regions labeled with centroids: A) Input image containing the forged region highlighted by a red rectangle, representing a "bird." I is illuminated by a contrast operation with parameter $c = 0.7$. B) Segmented regions in the mapped image. C) Centroids of small regions.

centroid is regarded as a central key point. For example, a bird object in a forged image (i.e., the input image shown in Fig. 4a) is detected by SRM, as illustrated in Fig. 4b. The centroid for the bird is as shown in Fig. 4c.

Color constancy based on multiscale retinex with a role of color distribution

Color can be an important cue for object recognition. Colors in an image can be innate assets of objects, as well as light sources. A forger always has the natural tendency to alter colors of the light source in duplicated regions. These effects of the light source between duplicated regions should undergo contrast enhancement and color correction [56]. Preprocessing the forged image based on color constancy is essential to achieve illumination-invariant forgery detection. Color constancy is applied by normalizing the lighting condition to an ideal estimated achromatic white light. The multiscale retinex (MSR) method was suggested by Pan et al. [57] to correct the chromaticity of the illuminant component in the input image. MSR is a nonlinear and context-dependent method applied to improve a color at an image intensity with the coordinates *(x, y)* as follows:

$$I(x, y) = L(x, y)\ .\ \ R(x, y), \tag{5}$$

Suppose that a given image I is decomposed into two parts as follows: (1) $R(x,y)$ is the reflectance at coordinate (x,y), and (2) L(x, y) is the illumination. The decomposition considers the logarithmic space as

$$\log I\ (x,\ \ y) = \log R(x,\ \ y) + \log L(x,\ \ y), \tag{6}$$

The MSR method can handle the input image with an arbitrary resolution based on multiple Gaussian filters with different weights W_k. It is defined as follows:

$$M_i\ (x, y) = \sum_{k=1}^{K} W_k{*}(\log I_i(x, y){-}log(\ F_k(x, y){*}I_i(x, y)), \tag{7}$$

$$F_k\ (x, y) = K\ e^{-(x^2+y^2)/\sigma_k^2}, \tag{8}$$

$$\iint F_k\ (x, y)\ dxdy = 1, \tag{9}$$

where $M_i(x, y)$ is the output of a retinex method based on the scale K. In our method, K represents a number of scales $=3$, W_k is the weighting value of every single retinex at scale k, σ_k is a scale parameter that controls the performance of the MSR algorithm, and $F_k(x, y)$ is the improved image defined as a result of the MSR algorithm. In this paper, we have used three Gaussian filters with small-, medium-, and large-scale values of K. These scales are utilized by MSR to approximate the local illuminant as shown in Fig. 5.

In this study, σ_k is a scale factor that changes the scale of an image. We applied the MSR algorithm to the original image, forged image, and segmented image, as shown in Fig. 6. A small σ_k affects the MSR output. The original image is improved to have fine features. A large σ_k improves the segmented image to provide color information. Fine features and color information of an image have inspired the MSR algorithm to enhance the forged image by calculating the average MSR of the image with three scaling factors.

MI-CSCT descriptor

To increase the discriminative power of features in the image, we propose an illumination-invariant descriptor for photometric transformations called MI-CSCT. This is a statistical model used in an adaptive window with a fixed size to handle sufficient information in the image. The adaptive window evaluates the variations in intensity and disparity in a certain compact region around the central pixel, comparing the central pixel with its local neighbors. The formula of MI-CSCT is defined as the number of pixels in that the adaptive window is greater than the intensity of the central pixel [58]. The MI-MCST descriptor creates an ordered stream of bits, where each given bit is normalized into *[0, 1]* when the central pixel and corresponding local pixels have the same relation. For example, for an image $I(x,y)$ with a scalar value at pixel location (x,y), an anisotropic Gaussian G_σ at scale σ filters the image regions. It can be defined by the following equation:

$$\hat{E}_j = I(x, y){*}G_j, \tag{10}$$

where $j\epsilon\{\sigma, x, y\}$ specifies either smooth or spatial differentiation. Each region is normalized by symmetric center census transform to provide illumination-invariant derivatives and suppress regional intensity variations. This is defined as

$$\xi(I_{j1}, I_{j2}) = \begin{cases} 1, & I_{j1} > I_{j2} \\ 0, & I_{j1} \le I_{j2} \end{cases}. \tag{11}$$

The result of the comparison function ξ is concatenated in a *bit* vector. It is defined as

$$TC_{m,n}(I_{(x,y)}) = \otimes_{i=-n'}^{n'} \otimes_{j=-m'}^{m'}\ \ \xi(I(x, y), I(x + i, y + j)), \tag{12}$$

where TC is applied to an image patch of $n \times m$ pixels instead of a circular region, $\otimes$ is a bitwise concatenation operator, and$n' = [n/2]$, *while* $m' = [m/2]$. Therefore, for window sizes of *3 x 3* and *5 x 5*, we can obtain efficient representations of *8-bit* and *24-bit* vectors, respectively.

While the original census transform (CT) [59] is a generalization of the gray value invariant, the modified census transform is created to offer some advantages, such as providing a disparity map, handling objects' structures, and being more robust to illumination by weighing each sample of the census transform by its Gaussian-based features. It is defined as follows:

$$\hat{w}_j = \frac{\xi_j}{\hat{E}_j}. \tag{13}$$

These promising features motivate us to investigate new generalizations of the census transform that can have excellent performance for detecting objects in the images and the capability of handling blocks with a saturated center value. Figure 7 presents the internal structure of an image, which is developed by two methods—MI-CSCT and CT. Figure 7a has more detailed features than Fig. 7b does. It can be observed that the MI-CSCT descriptor gives a more precise separation between regions in the image.

To improve the discriminative power of the descriptor, the

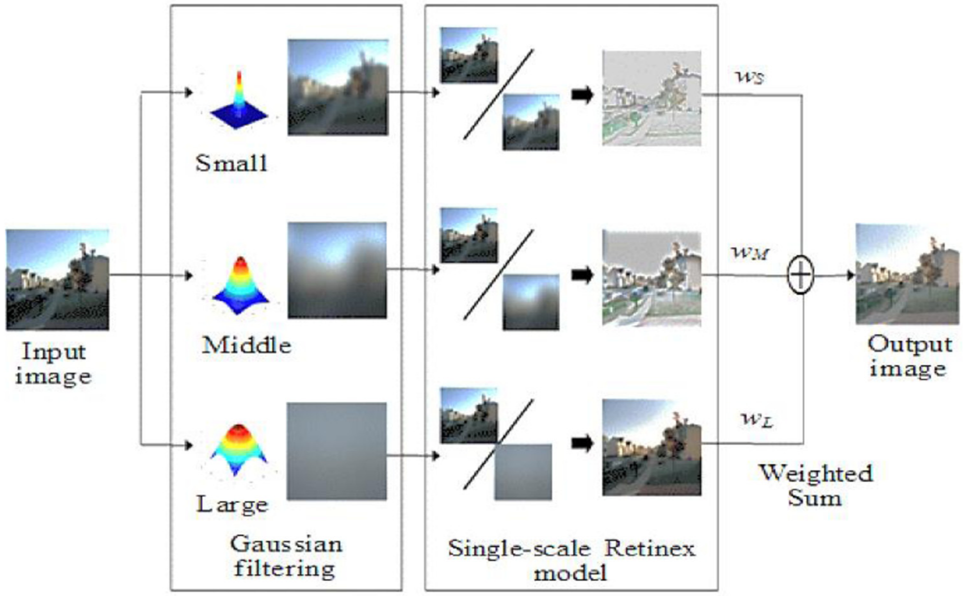


Fig. 5. MSR algorithm where $\sigma_{small} = 0.5$, $\sigma_{middle} = 2.5$, and $\sigma_{large} = 12.5$, while K represents *3 scales*.

incorporation of integral images is necessary. The integral image at pixel location (x, y) is defined as the sum of the intensity values for all pixels in the image with a location less than or equal to *(x, y)*. The integral image is defined efficiently by cumulative raw sum operation as follows:

$$\hat{w}'_{i,j} = \sum_{k=1}^{i} \hat{w}_{k,j}, \tag{14}$$

Where $\hat{w}'_{i,j}$ is the integral region. We use the effects of weighted CT in distance measure to apply an efficient matching between duplicated regions. As a result, the image can have various segmented regions, where each has a centroid. We select a *4 x 4* block around each centroid. The MI-CSCT descriptor is extracted for each block to produce integral region $\hat{w}'_{i,j}$.

Clustering duplicated regions based on adaptive FCM

The main goal of the clustering step is to detect duplicated regions in the forged image to improve its detection accuracy. The adaptive FCM algorithm was proposed by Kaufmann et al. [60] to group matched local regions together. AFCM follows an iterative process to obtain clusters and fuzzy cluster memberships by minimizing the following objective function:

$$J_m = \sum_{i=1}^{C} \sum_{j=1}^{N} u_{ij}^{m} |\hat{w}'_j - v_i|. \tag{15}$$

Let $\hat{w}' = (\hat{w}'_1, \hat{w}'_2, \ldots, \hat{w}'_N)$ denote an integral image with N regions to be clustered into c clusters. Here, $v_i = (1, 2, \ldots, c)$ is the cluster center of the i^{th} cluster, while u_{ij} represents a membership matrix of region $\hat{w}'_j$ belonging to the i^{th} cluster, and $m \in [1, \infty)$ is the weighting exponent that controls the fuzziness of the resulting partition. In addition, N is the number of input regions saved into feature vectors, c is the number of clusters, and $|.|$is a straightforward sum of absolute distance (SAD). It is the dissimilarity measure proposed by Li et al. [61].

Results and Discussion

Region duplication forgery benchmarks

Two standard benchmarking image datasets are used in our

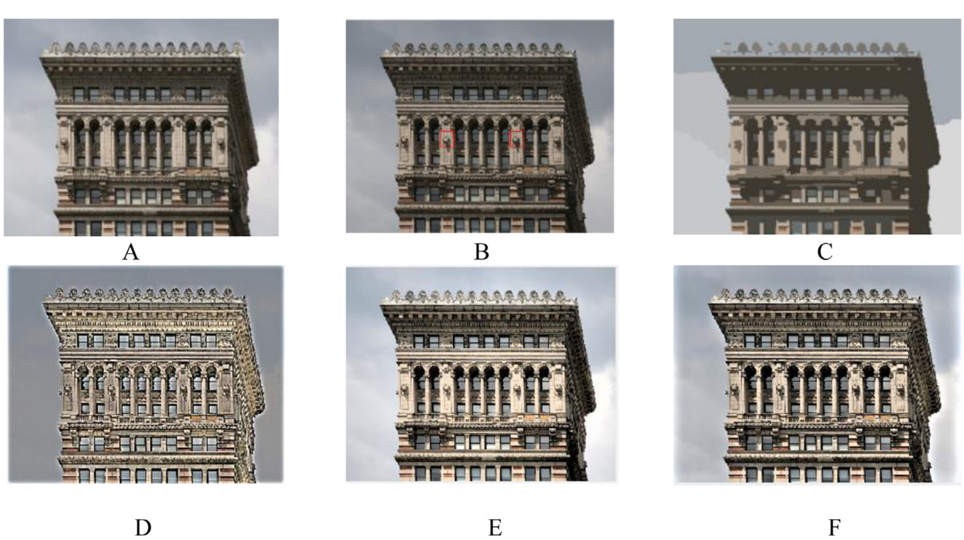


Fig. 6. Results of the automatic MSR algorithm for enhancement of images in wide-ranging lighting conditions: A) original image, B) forged image, C) segmented forged image. Enhanced images: D) enhanced image by color correction based on MSR with $\sigma_{small} = 0.5$; E) enhanced image by color correction based on MSR with $\sigma_{middle} = 2.5$; F) enhanced image by color correction based on MSR with $\sigma_{large} = 5$.

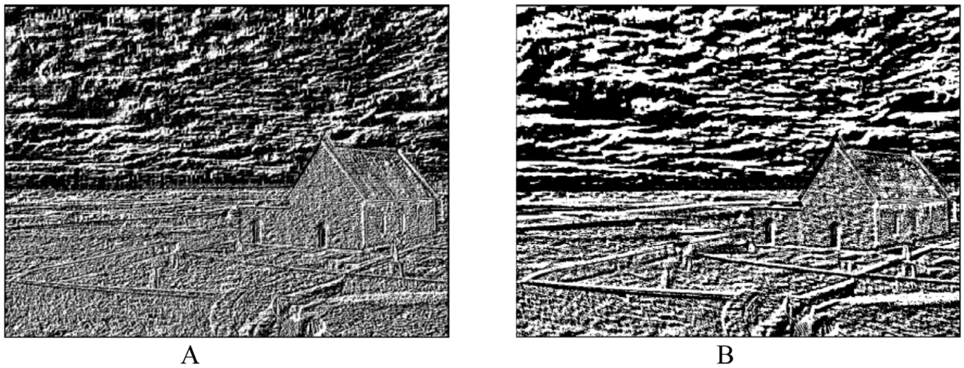


Fig. 7. Results of census transforms using two algorithms : A) MI-CSCT and B) CT [59].

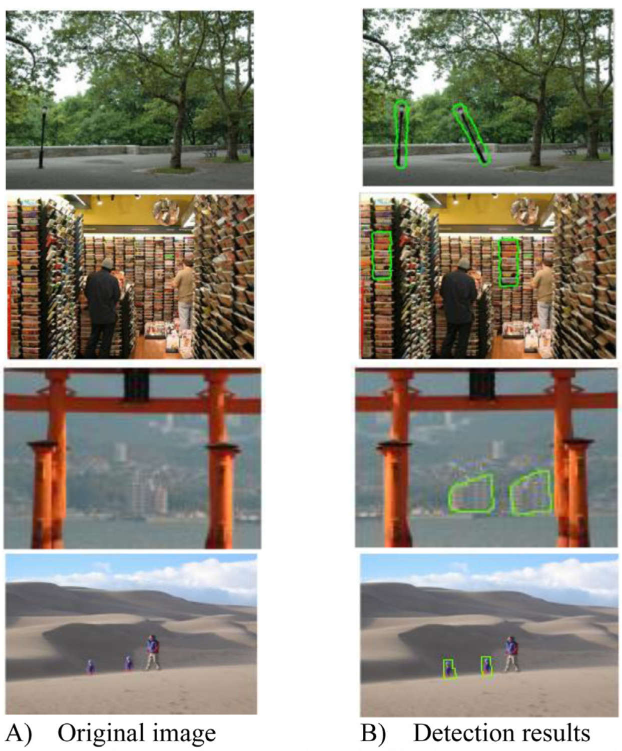


Fig. 8. Detection results of region duplication forgery in the MICC-F200, F220, and F600 datasets.

Table 1
Detection rates of region duplication forgery detection using image manipulation datasets [13].

Block size	4 x 4	8 x 8	16 x 16	32 x 32
F_c	0.966	0.954	0.943	0.872
F_f	0.02	0.03	0.03	0.185

experiments, namely, Media Integration and Communication Center (MICC) dataset [28] and Image Data Manipulation [13]. We have selected different types of images that include forged regions. MICC includes the image subsets MICC-F2000, MICC-F220, MICC-F8multi, and MICC-F600. They contain about 2,000, 220, 8, and 600 forged images, respectively. Image data manipulation consists of 48 images in the PNG color format. The forged images from these datasets are tested according to illumination changes, JPEG compression, and additive white Gaussian noise (AWGN). We have resized the large images to 500 *x* 333 pixels to reduce the computational cost.

The main goal is to evaluate the performance of our method at the block level against illumination variations. The experiments examine the performance of the proposed method through *158* images. Moreover, they have two types of forged regions—non-uniform regions and uniform regions—as shown in Fig. 8.

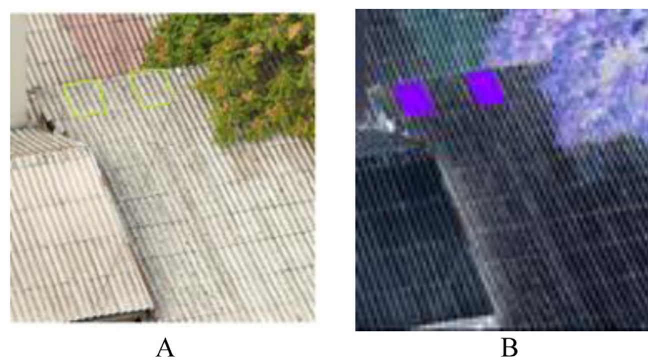


Fig. 9. Detection of forged regions while duplicated region was manipulated by brightness into the range [0.01, 0.8]. A) Forged image with duplicated regions. B) Detection result.

Table 2
Illumination analysis: average F_c and F_f rates under various block sizes.

Illumination variations	Block size	4 x 4	8 x 8	16 x 16	32 x 32
[0.01,0.95]	F_c	0.974	0.968	0.920	0.920
	F_f	0.042	0.045	0.052	0.077
[0.01, 0.9]	F_c	0.962	0.952	0.922	0.922
	F_f	0.050	0.050	0.072	0.072
[0.01, 0.8]	F_c	0.933	0.932	0.910	0.910
	F_f	0.055	0.055	0.074	0.074

Table 3
Comparison of our method against other methods.

Methods	*P*	*R*	F_{score}
[62]	0.7188	0.9583	0.8214
[63]	0.9167	0.9286	0.9512
[64]	0.8936	0.8750	0.8842
Our method	0.9634	0.8914	0.9260

Performance evaluation

An *F-score* was used to evaluate the detection of forged regions at the pixel level. To illustrate the performance of the proposed method, we used two main criteria (F_c and F_f). F_c represents correct detection, and F_f represents false detection rates. They are computed using the following equations:

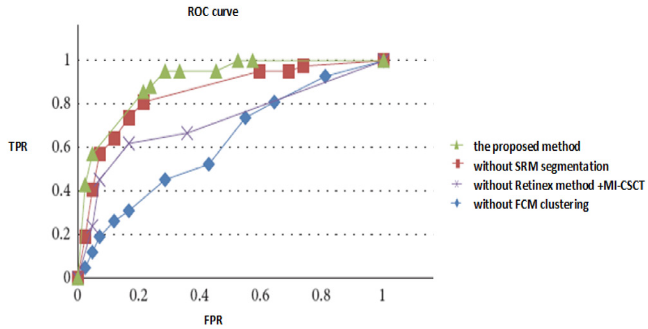


Fig. 10. ROC curve of the proposed method under illumination changes.

$$F_c = \frac{|C \cap \bar{C}| + |T \cap \bar{T}|}{|C| + |T|}, \tag{16}$$

$$F_f = \frac{|\bar{C} - C| + |\bar{T} - T|}{|\bar{C}| + |\bar{T}|}, \tag{17}$$

where C is the original region copied by the forger and T is the forged region moved to a new area within the image. $\bar{C}$ is the perceived copied region, and $\bar{T}$ is the perceived forged region. F_c represents the performance of the proposed method in terms of detecting blocks inside duplicated areas of the image, while F_f reflects the number of blocks that are not part of the forged region and are incorrectly localized by our method. In the experiments, the block sizes of the segmented region were set as $B = 4 x 4, 8 x 8, and 16 x 16$. The block similarity threshold was $t_{similarity} = 0.07$. Table 1 shows the forgery detection rates of the proposed method based on various block sizes. F_c is 0.96 and F_f is approximately *0.03*. The proposed method yields promising results with block sizes of *4 x 4, 8 x 8, and 16 x 16*. F_c is decreased to *0.87* and gives a higher value of $F_f = 0.185$ when the block size is *32 x 32*. The areas of the forged images were observed to be small, and they cannot be localized by our method when using a larger block size.

Performance of the proposed method against illumination changes

In two image datasets, MICC-F2000 and image data manipulation, the forged region was manipulated by changing the intensities of the forged region in the range *[0–1]*. Three intervals of brightness were utilized to make forgeries as follows: *[0.01, 0.95]*, *[0.01, 0.9]*, and *[0.01, 0.8]*. While brightness *[0.01, 0.95]* was used in the forged region, it can be noticed that this change is imperceptible. Brightness variations of *[0.01, 0.8]* are visually detectable. Figure 9 shows an example of a forged image that was distorted by changing the brightness into the range *[0.01, 0.8]*, with its corresponding detection results. Table 2 presents the average performance of the proposed method in terms of detection rates, F_c and F_f, against illumination changes.

Comparison

To evaluate the proposed method, it was compared with others according to three evaluation metrics at the image level, namely, precision P, recall R, and F_{score}, as defined in [28, 29]. When P, R, and F_{score} are close to 1, it means a higher performance of the detection method, as shown in Table 3, where $P = 0.9634$, $R = 0.8914$, and $F_{score} = 0.9260$. Some existing methods [62-64] were compared with the proposed method, as presented in Table 3. This table gives the statistical analysis of the method under region duplication forgery on the image manipulation dataset.

The proposed method was validated by removing the SRM segmentation. Figure 10 shows that the SRM method positively contributes to detection accuracy. In the receiver operating characteristic (ROC) curve, the average *TPR* decreased to *0.80*, and the *FPR* increased to *0.6–0.7*. Furthermore, in the proposed method without the retinex method and MI-CSCT, color correction on the image regions was not employed to enhance the image. This made it difficult for the proposed method to detect any matched forged regions accurately. As shown in the ROC curve, the detection accuracy of the proposed method without adaptive FCM was quite low, as *TPR* was *0.6* and *FPR* was *0.2*.

Conclusion

The proposed method starts by splitting an image into homogeneous regions using SRM segmentation to detect small regions of images. These regions are improved by MSR with color distribution to represent their fine features. These features are normalized using MI-CSCT descriptor in the domain of the illumination variations. Experimental results show that the proposed method can detect two types of forged regions: uniform and non-uniform regions. The performance of our method is evaluated by using matrices precision, recall and F_{score}. According to ROC curve, it is observed that FPR is decreased due to employing adaptive FCM. Future direction of our research is estimating illumination parameters for the forged duplicated regions.

Acknowledgment

The authors are grateful to the University of Ha'il, Ha'il, Kingdom of Saudi Arabia for supporting this research.

References

[1] Y. Huo, H. He, and F. Chen, "A semi-fragile image watermarking algorithm with two-stage detection," Multimedia Tools and Applications, pp. 1-27, 2013/01/05 2013.
[2] S. Dadkhah, M. Köppen, H.A. Jalab, S. Sadeghi, A.A. Manaf, D.M. Uliyan, Electromagnetismlike Mechanism Descriptor with Fourier Transform for a Passive Copy-move Forgery Detection in Digital Image Forensics, ICPRAM (2017) 612–619.
[3] S. Sadeghi, H.A. Jalab, K. Wong, D. Uliyan, S. Dadkhah, Keypoint based authentication and localization of copy-move forgery in digital image, Malaysian Journal of Computer Science 30 (2) (2017) 117–133 volno.
[4] H. Farid, Image forgery detection, Signal Processing Magazine, IEEE 26 (2) (2009) 16–25 volno.
[5] O.M. Al-Qershi, B.E. Khoo, Passive detection of copy-move forgery in digital images: State-of-the-art, Forensic science international 231 (1) (2013) 284–295 volno.
[6] P. Sutthiwan, Y.Q. Shi, Anti-Forensics of double JPEG compression detection, Digital Forensics and Watermarking, Springer, 2012, pp. 411–424.
[7] C.-T. Li, Source camera identification using enhanced sensor pattern noise, Information Forensics and Security, IEEE Transactions on 5 (2) (2010) 280–287 volno.
[8] M.K. Johnson, H. Farid, Exposing digital forgeries by detecting inconsistencies in lighting, Proceedings of the 7th workshop on Multimedia and security, ACM, 2005, pp. 1–10.
[9] M.K. Johnson, H. Farid, Detecting photographic composites of people, Digital Watermarking, Springer, 2008, pp. 19–33.
[10] S. Avidan, A. Shamir, Seam carving for content-aware image resizing, ACM Transactions on graphics (TOG) 26 ACM, 2007, p. 10 volno.
[11] I.-C. Chang, C.-J. Hsieh, Image Forgery Using An Enhanced Bayesian Matting Algorithm, Intelligent Automation & Soft Computing 17 (2) (2011) 269–281 volno.
[12] R. Granty, T. Aditya, S. Madhu, Survey on passive methods of image tampering detection, Communication and Computational Intelligence (INCOCCI), 2010 International Conference on, IEEE, 2010, pp. 431–436.
[13] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," 2012.
[14] vol, H. Li, J. Zheng, Blind Detection of Digital Forgery Image Based on the Edge Width, in: Y. Zhang, Z.-H. Zhou, C. Zhang, Y. Li (Eds.), Intelligent Science and Intelligent Data Engineering, 7202 Lecture Notes in Computer Science: Springer Berlin Heidelberg, 2012, pp. 546–553 volEds..
[15] D.M. Uliyan, H.A. Jalab, A.W.A. Wahab, P. Shivakumara, S. Sadeghi, A novel forged blurred region detection system for image forensic applications, Expert Systems with Applications 64 (2016) 1–10 vol.
[16] A. Roy, R. Dixit, R. Naskar, R.S. Chakraborty, Copy-Move Forgery Detection in Digital Images—Survey and Accuracy Estimation Metrics, Digital Image Forensics, Springer, 2020, pp. 27–56 pp.
[17] S. Devi Mahalakshmi, K. Vijayalakshmi, S. Priyadharsini, Digital image forgery detection and estimation by exploring basic image manipulations, Digital Investigation 8 (3) (2012) 215–225 volno.
[18] S. Teerakanok, T. Uehara, Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis, IEEE Access 7 (2019) 40550–40568 vol.
[19] N.B.A. Warif, et al., Copy-move forgery detection: survey, challenges and future directions, Journal of Network and Computer Applications 75 (2016) 259–278 vol.

[20] G. Liu, J. Wang, S. Lian, Y. Dai, Detect image splicing with artificial blurred boundary, Mathematical and Computer Modelling 57 (11) (2013) 2647–2659 volno.
[21] J. Wang, G. Liu, B. Xu, H. Li, Y. Dai, Z. Wang, Image Forgery Forensics Based on Manual Blurred Edge Detection, Multimedia Information Networking and Security (MINES), 2010 International Conference on, IEEE, 2010, pp. 907–911.
[22] D. Uliyan, M.A. Abushariah, A.M. Altamimi, Blur Invariant Features For Exposing Region Duplication Forgery Using ANMS And Local Phase Quantization, Informatica 42 (4) (2018) volno.
[23] T. Wang, J. Tang, B. Luo, Blind detection of region duplication forgery by merging blur and affine moment invariants, Image and Graphics (ICIG), 2013 Seventh International Conference on, IEEE, 2013, pp. 258–264.
[24] B. Fan, F. Wu, Z. Hu, Rotationally invariant descriptors using intensity order pooling, Pattern Analysis and Machine Intelligence, IEEE Transactions on 34 (10) (2012) 2031–2045 volno.
[25] R. Davarzani, K. Yaghmaie, S. Mozaffari, M. Tapak, Copy-move forgery detection using multiresolution local binary patterns, Forensic Science International 231 (1) (2013) 61–72 volno.
[26] T.J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, A. de Rezende Rocha, Exposing digital image forgeries by illumination color classification, Information Forensics and Security, IEEE Transactions on 8 (7) (2013) 1182–1194 volno.
[27] H.A. Alberry, A.A. Hegazy, G.I. Salama, A fast SIFT based method for copy move forgery detection, Future Computing and Informatics Journal 3 (2) (2018) 159–165 volno.
[28] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A sift-based forensic method for copy–move attack detection and transformation recovery, Information Forensics and Security, IEEE Transactions on 6 (3) (2011) 1099–1110 volno.
[29] X. Pan, S. Lyu, Region duplication detection using image feature matching, Information Forensics and Security, IEEE Transactions on 5 (4) (2010) 857–867 volno.
[30] L. Chen, W. Lu, J. Ni, W. Sun, J. Huang, Region duplication detection based on Harris corner points and step sector statistics, Journal of Visual Communication and Image Representation 24 (3) (2013) 244–254 volno.
[31] L. Zheng, Y. Lei, G. Qiu, J. Huang, Near-duplicate image detection in a visually salient riemannian space, Information Forensics and Security, IEEE Transactions on 7 (5) (2012) 1578–1593 volnopp.
[32] D.M. Uliyan, M.A.F. Al-Husainy, A.M. Altamimi, H.A. Jalab, A forensic scheme for revealing post-processed region duplication forgery in suspected images, Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 10 (3) (2018) 37–45 volno.
[33] W.N. Nathalie Diane, S. Xingming, F.K. Moise, A Survey of Partition-Based Techniques for Copy-Move Forgery Detection, The Scientific World Journal 2014 (2014).
[34] M. Zimba, S. Xingming, DWT-PCA(EVD) Based Copy-move Image Forgery Detection, International Journal of Digital Content Technology and its Applications 5 (1) (2011).
[35] Y. Cao, T. Gao, L. Fan, Q. Yang, A robust detection algorithm for copy-move forgery in digital images, Forensic science international 214 (1) (2012) 33–43.
[36] P. Kakar, N. Sudha, Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features, Information Forensics and Security, IEEE Transactions on 7 (3) (2012) 1018–1028.
[37] D.M. Uliyan, H.A. Jalab, A. Abuarqoub, M. Abu-Hashem, Segmented-Based Region Duplication Forgery Detection Using MOD Keypoints and Texture Descriptor, Proceedings of the International Conference on Future Networks and Distributed Systems, ACM, 2017, p. 6.
[38] H. Shao, T. Yu, M. Xu, W. Cui, Image region duplication detection based on circular window expansion and phase correlation, Forensic science international 222 (1) (2012) 71–82.
[39] W. Li, N. Yu, Rotation robust detection of copy-move forgery, Image Processing (ICIP), 2010 17th IEEE International Conference on, IEEE, 2010, pp. 2113–2116.
[40] A. Myrna, M. Venkateshmurthy, C. Patil, 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 3 IEEE, 2007, pp. 371–377.
[41] A.V. Malviya, S.A. Ladhake, Pixel based image forensic technique for copy-move forgery detection using auto color correlogram, Procedia Computer Science 79 (2016) 383–390.
[42] B. Harjito, H. Prasetyo, Passive copy-move forgery detection using halftoning-based block truncation coding feature, Journal of Physics: Conference Series 855 IOP Publishing, 2017012016.
[43] J.-M. Guo, Y.-F. Liu, Z.-J. Wu, Duplication forgery detection using improved DAISY descriptor, Expert Systems with Applications (2012).
[44] S. Bayram, H.T. Sencar, N. Memon, An efficient and robust method for detecting copy-move forgery, Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, IEEE, 2009, pp. 1053–1056.
[45] S. Bravo-Solorio, A.K. Nandi, Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics, Signal Processing 91 (8) (2011) 1759–1770.
[46] B. Mahdian, S. Saic, Using noise inconsistencies for blind image forensics, Image and Vision Computing 27 (10) (2009) 1497–1503.
[47] N. Muhammad, M. Hussain, G. Muhamad, G. Bebis, A non-intrusive method for copy-move forgery detection, Advances in Visual Computing, Springer, 2011, pp. 516–525.
[48] S. Battiato, G.M. Farinella, E. Messina, G. Puglisi, Robust image alignment for tampering detection, Information Forensics and Security, IEEE Transactions on 7 (4) (2012) 1105–1117.
[49] X. Bo, W. Junwen, L. Guangjie, D. Yuewei, Image copy-move forgery detection based on SURF, Multimedia Information Networking and Security (MINES), 2010 International Conference on, IEEE, 2010, pp. 889–892.
[50] B. Shivakumar, L.D.S.S. Baboo, Detection of region duplication forgery in digital images using SURF, IJCSI International Journal of Computer Science Issues 8 (4) (2011).
[51] D. Uliyan, H. Jalab, A. Abdul Wahab, S. Sadeghi, Image region duplication forgery detection based on angular radial partitioning and Harris key-points, Symmetry 8 (7) (2016) 62.
[52] D.G. Lowe, Distinctive image features from scale-invariant keypoints, International journal of computer vision 60 (2) (2004) 91–110.
[53] G. Muhammad, M.H. Al-Hammadi, M. Hussain, A.M. Mirza, G. Bebis, Copy move image forgery detection method using steerable pyramid transform and texture descriptor, EUROCON, 2013 IEEE, IEEE, 2013, pp. 1586–1592.
[54] R. Nock, F. Nielsen, Statistical region merging, Pattern Analysis and Machine Intelligence, IEEE Transactions on 26 (11) (2004) 1452–1458.
[55] F. Nielsen, R. Nock, On region merging: The statistical soundness of fast sorting, with applications, 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings. 2 IEEE, 2003, pp. II–19.
[56] H.R.V. Joze, M.S. Drew, Exemplar-based color constancy and multiple illumination, Pattern Analysis and Machine Intelligence, IEEE Transactions on 36 (5) (2014) 860–873.
[57] S. Pan, X. An, H. He, Adapting iterative Retinex computation for high-dynamic-range tone mapping, Journal of Electronic Imaging 22 (2) (2013) 023006.
[58] D. Hafner, O. Demetz, J. Weickert, Why Is the Census Transform Good for Robust Optic Flow Computation? Springer, 2013.
[59] R. Zabih, J. Woodfill, Non-parametric local transforms for computing visual correspondence, Computer Vision—ECCV'94, Springer, 1994, pp. 151–158.
[60] A. Kaufmann, Theory of expertons and fuzzy logic, Fuzzy Sets and Systems 28 (3) (1988) 295–304.
[61] Z. Li, J. Yuan, W. Zhang, Fuzzy C-mean algorithm with morphology similarity distance, 2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery 3 IEEE, 2009, pp. 90–94.
[62] M. Zandi, A. Mahmoudi-Aznaveh, A. Talebpour, Iterative copy-move forgery detection based on a new interest point detector, IEEE Transactions on Information Forensics and Security 11 (11) (2016) 2499–2512.
[63] D. Cozzolino, G. Poggi, L. Verdoliva, Efficient dense-field copy–move forgery detection, IEEE Transactions on Information Forensics and Security 10 (11) (2015) 2284–2297.
[64] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, G. Serra, Copy-move forgery detection and localization by means of robust clustering with J-Linkage, Signal Processing: Image Communication 28 (6) (2013) 659–669.