Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 619564, 12 pages
http://dx.doi.org/10.1155/2013/619564

Research Article

Passive Forensics for Region Duplication Image Forgery Based on Harris Feature Points and Local Binary Patterns

Jie Zhao[1,2] and Weifeng Zhao[1]

[1] *School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China*
[2] *School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China*

Correspondence should be addressed to Jie Zhao; zhaoj@tju.edu.cn

Received 7 November 2013; Revised 3 December 2013; Accepted 4 December 2013

Academic Editor: Ebrahim Momoniat

Nowadays the demand for identifying the authenticity of an image is much increased since advanced image editing software packages are widely used. Region duplication forgery is one of the most common and immediate tampering attacks which are frequently used. Several methods to expose this forgery have been developed to detect and locate the tampered region, while most methods do fail when the duplicated region undergoes rotation or flipping before being pasted. In this paper, an efficient method based on Harris feature points and local binary patterns is proposed. First, the image is filtered with a pixelwise adaptive Wiener method, and then dense Harris feature points are employed in order to obtain a sufficient number of feature points with approximately uniform distribution. Feature vectors for a circle patch around each feature point are extracted using local binary pattern operators, and the similar Harris points are matched based on their representation feature vectors using the BBF algorithm. Finally, RANSAC algorithm is employed to eliminate the possible erroneous matches. Experiment results demonstrate that the proposed method can effectively detect region duplication forgery, even when an image was distorted by rotation, flipping, blurring, AWGN, JPEG compression, and their mixed operations, especially resistant to the forgery with the flat area of little visual structures.

1. Introduction

Nowadays, with the development of state-of-the-art digital image technologies and the widespread use of powerful image editing software, even people who are not experts in image processing can fake an image easily without leaving any visual tampering clues. Digital image forgeries, which seriously debase the credibility of photographic images as definite records of events, have become so widespread a problem that affects social and legal systems, forensic investigations, intelligence services, and security and surveillance systems. In order to recover people's confidence in the authenticity of digital images, image forensics aiming to reveal forgery operations in digital images are receiving more and more attention.

In recent years, many image forgery detection techniques have been proposed, which can be broadly classified into two categories: active approach and passive approach. Active image forensic techniques represented by digital watermark [1, 2] require prior knowledge about the original image, thus they are not automatic. In addition, the drawback of digital watermark is that an imperceptible digital code (a watermark) must be inserted at the time of recording, which would restrict this approach to specially equipped digital cameras. In contrast, passive forensics aims at identifying the authenticity of an image without prior knowledge and in the absence of watermarks, which works by assuming that even though the tampered images do not reveal any visual artifacts, the underlying statistics of these images would be distinct from the original ones. Owing to its incomparable advantage, passive image forensics has been regarded as the promising research interest in the field of image forensics.

Among forgery techniques using typical image processing tools, region duplication, also being called copy-move, is the most common type of image forgery where a region of an image is copied and then pasted to another nonintersecting region in the same image to conceal an important element or to emphasize a particular object. Due to the nature of region duplication forgery, there will be at least two similar regions in the tampered image, which is not

common in natural images and thus can be used to detect this specific artifact. In [3], Weiqi et al. proposed the model of region duplication forgery on which most existing detection methods are based. Since duplicated regions come from the same image, they have similar properties like texture, color, and noise. In practical situations, however, several image intermediate operations and postprocessing operations could be involved in practical region duplication forgery. The intermediate operations could be rotation, flipping, scaling, or illumination modifying. The postprocessing operations include noise adding, JPEG compression, or blurring. In a practical situation, a faked image may be a combination of two or more operations, which is a direct challenge to most existing techniques.

In this paper, we propose a passive detection scheme for region duplication image forgery based on Harris corner points and local binary patterns. Experiment results show that the proposed method can effectively detect region duplication forgery, even when an image was distorted by rotation, flipping, blurring, AWGN, JPEG compression, and their mixed operations, especially resistant to the forgery with the flat area of little visual structures.

The rest of the paper is organized as follows. In Section 2, the related works on region duplication forgery detection are introduced. Section 3 briefly reviews Harris corner points and local binary patterns. In Section 4, the proposed algorithm is described in detail. The experimental results are given and the corresponding analysis is discussed in Section 5. The conclusion is drawn in Section 6.

2. Related Works

In the last decade, many passive techniques for region duplication forgery have been proposed, which could be grouped into two categories: block-based methods [3–10] and keypoint-based methods [11–15]. Fridrich et al. [4] first analyzed the exhaustive search and then proposed a block matching detection scheme based on quantized Discrete Cosine Transform (DCT) coefficients. In order to make this algorithm more robust and efficient, Huang et al. [9] and Cao et al. [10] proposed an improved DCT-based detection method, respectively, which reduced the dimension of feature vector. Popescu and Farid [5] proposed a similar method which represented image blocks using Principal Component Analysis (PCA) instead of DCT. Weiqi et al. [3] extracted color features as well as special intensity ratio to represent a block characteristics vector. A different approach was presented by Xiaobing and Shengmin [6] in which the features were represented by the Singular Value Decomposition (SVD). Guohui et al. [7] proposed to decompose the image into four subbands using Discrete Wavelet Transform (DWT) and then apply SVD on the blocks. However, when images are manipulated through geometry transforms like rotation, flipping, or scaling, all these above-mentioned methods cease to be effective. To address this problem, Bayram et al. [8] applied Fourier-Mellin Transform (FMT) to each block and FMT values were finally projected to one dimension to form the feature vector. However, FMT-based method can only detect duplicated regions with slight rotation according to their experimental results. Bravo-Solorio and Nandi [16] proposed a scheme based on log-polar coordinates to detect forgery regions, even when the duplicated regions have undergone flipping, rotation, and scaling. Nevertheless, since the method depends on the pixel values, it is sensitive to the change of the pixel values. Almost all the methods above-mentioned are block-based which attempt to find an effective and robust representation of each block, moreover, they are expected to be insensitive to common postprocessing operations and intermediate operations.

In contrast to block-based methods, keypoint-based methods rely on the identification and selection of high-entropy image regions. In [11–13], some approaches that extracted keypoints by Scale-Invariant Feature Transform (SIFT) were proposed to detect the forgery due to their robustness to several geometrical transforms such as rotation and scaling. However, SIFT-based scheme still has a limitation on detection performance since it is only possible to extract the keypoints from peculiar points of the image and not robust to some postprocessing operations like blurring and flipping based on our experimental results. Xu et al. [14] and Shivakumar and Baboo [15] proposed another keypoint-based method which used Speeded Up Robust Features (SURF) to approximately show the duplicated regions in the forged images. The main drawback of most keypoint-based methods is that copied regions are often only sparsely covered by matched keypoints. Thus they do not provide the exact extent and location of the detected duplicated region but only display the matched keypoints. Furthermore, if the copied region exhibits little structure, it may happen that the region is completely missed [17].

Most existing methods are typically evaluated against simple forgeries where human viewers have no trouble to identify the duplicated regions or low resolution images which are a far cry from realistic tampered images with high resolution. Their detection performance on challenging realistic forgery images is far from certain.

3. Theoretical Background

3.1. Harris Corner Detector. Harris corner detector [18] is a widely used interest point detector, which has been applied successfully in several image processing [19, 20] and robotic vision [21, 22] applications, since Harris feature points are stable under majority of the attacks such as rotation, noise adding, and illumination change. Harris corner detector is based on an underlying assumption that feature points are associated with maxima of the local autocorrelation function.

For a given image $I(x, y)$, its autocorrelation matrix M at point (x, y) can be calculated as follows:

$$M(x, y) = \sum_{u,v} w(u, v) \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix}, \quad (1)$$

where I_x and I_y are the respective derivatives of pixel intensity in the x and y directions at point (x, y). $w(u, v)$ is

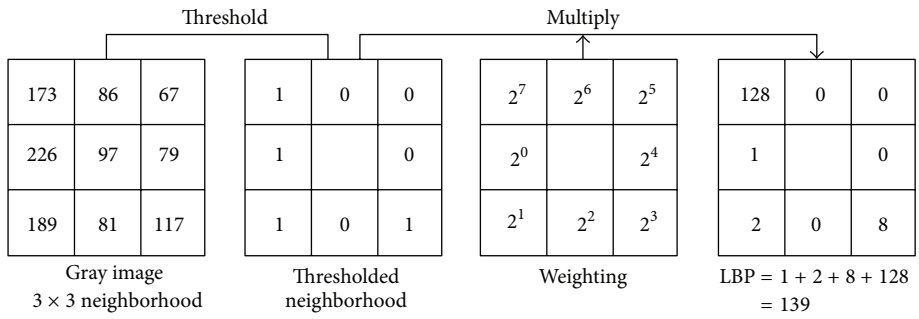


Figure 1: Calculation of the original LBP operator.

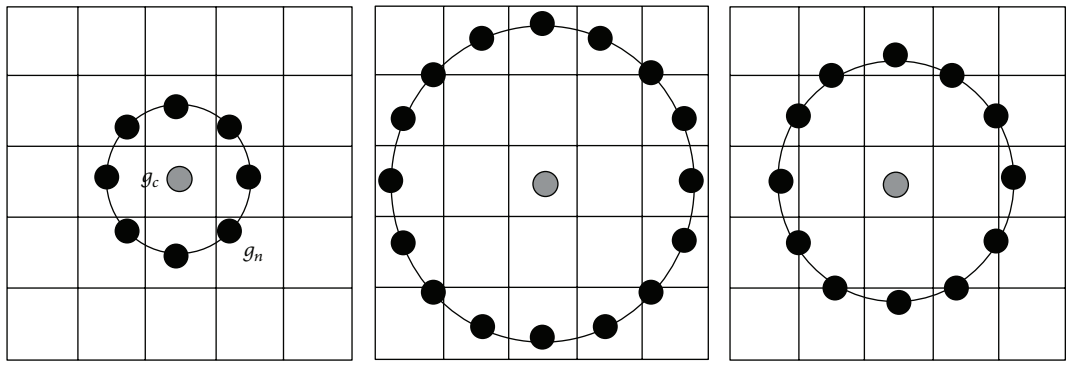


Figure 2: Circularly symmetric neighborhoods for different P and R, and ($P = 8$, $R = 1$), ($P = 16$, $R = 2$), ($P = 12$, $R = 1.5$).

the weighting function usually of circular Gaussian form as follows:

$$w(u, v) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{u^2 + v^2}{2\sigma^2}\right). \tag{2}$$

Harris proposed a measure response R to detect corners of an image:

$$R = \det(M) - k \times \mathrm{tr}^2(M), \tag{3}$$

where $\det(\cdot)$ is the determinant, $\mathrm{tr}(\cdot)$ is the trace, and k is a scalar value empirically chosen from the range $[0.04, 0.06]$. Corner points which are greater than a specified threshold are identified as local maxima of the Harris measure response as follows:

$$\{(x_c, y_c)\} = \{(x_c, y_c) \mid R(x_c, y_c) > R(x_i, y_i), \\ \forall (x_i, y_i) \in W(x_c, y_c), R(x_c, y_c) > T\}, \tag{4}$$

where $\{(x_c, y_c)\}$ is the set of all corner points, $R(x, y)$ is the Harris measure response calculated at point (x, y), $W(x_c, y_c)$ is an 8-neighbor set centered around the point (x_c, y_c), and T is a specified threshold.

In the process of Harris feature points extraction, the threshold T determines the number of Harris feature points. The larger the value is, the less the number of feature points is. On the contrary, the smaller the value is, the greater the number of feature points is, and the more intensive they are distributed. In order to make the proposed algorithm effective even when the duplicated region is in the flat area with little visual structure or of small size, we propose to employ the dense Harris feature points, namely, the threshold T equal to zero, so that a large number of Harris feature points are obtained with approximately uniform distribution, which is more beneficial to enhance the robustness of the algorithm.

3.2. Local Binary Pattern. Local Binary Pattern (LBP), proposed by Ojala et al. [23], is a powerful means of texture description, which has gained increasing attention in many image analysis applications in virtue of its low computational complexity, invariance to monotonic grayscale changes and texture description ability. The LBP operator can be seen as a unified approach to statistical and structural texture analysis, since it describes each pixel by the relative gray levels of its neighboring pixels. Figure 1 illustrates the calculation of the original LBP for one pixel with a 3×3 neighboring block. These eight neighbors are labeled by thresholding with the central pixel value, weighted with powers of two, and then summed to obtain a new value assigned to the central pixel.

Using circular neighborhoods and linearly interpolation, LBP can be extended to allow the choice of any radius R and number of pixels in the neighborhood P to form a (P, R) neighborhood, illustrated in Figure 2. Denote the central pixel at position (x_c, y_c). Having P equally spaced

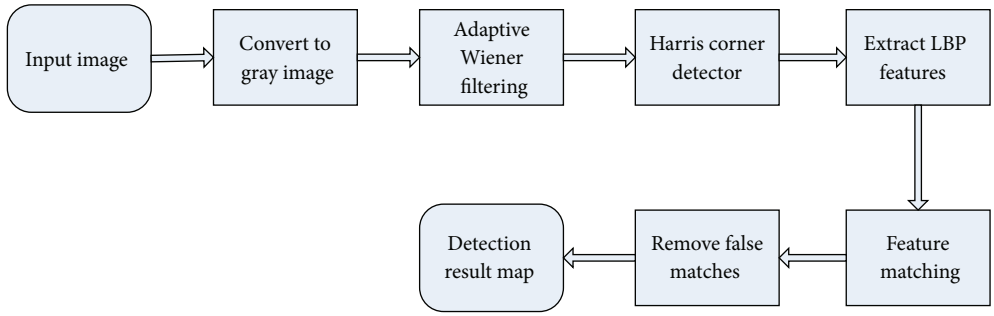


Figure 3: The flow diagram of the proposed detection method.

neighborhood pixels on a circle of radius R, LBP is calculated by:

$$\mathrm{LBP}_{P,R}(x_c, y_c) = \sum_{n=0}^{P-1} s(g_n - g_c)\, 2^n, \qquad s(x) = \begin{cases} 1, & x \geq 0, \\ 0, & x < 0, \end{cases} \tag{5}$$

where g_c and g_n correspond to the gray value of central pixel and neighboring pixel respectively.

For a given image with the size of $M \times N$, the normalized histogram of LBP codes is commonly used as a feature vector, which is computed over the whole image by:

$$H(\mathrm{bin}) = \left(\frac{1}{M \times N}\right) \sum_{i=1}^{M} \sum_{j=1}^{N} f(\mathrm{LBP}_{P,R}(i, j), \mathrm{bin}), \quad \mathrm{bin} \in [0, T], \tag{6}$$

$$f(x, y) = \begin{cases} 1, & x = y, \\ 0, & \text{otherwise}, \end{cases} \tag{7}$$

where T is the maximal LBP pattern value.

The final LBP feature of an image consists of computing the LBP code for each pixel within the image and building a histogram based on these codes. LBP feature is a good local image region descriptor, since it is very fast to calculate, and is invariant to monotonic illumination changes. However, the drawback of the LBP feature lies in the high dimensionality of histograms produced by the LBP codes [24]. Let P be the total number of neighboring pixels, then the LBP feature will have 2^P distinct values, resulting in a 2^P-dimensional histogram. A popular dimensionality reduction method for LBP is "uniform patterns," proposed by Ojala et al. in [23], and it is considered to convey some fundamental properties of texture. A local binary pattern is called uniform, denoted as $\mathrm{LBP}^{u2}_{P,R}$, if it contains at most two bitwise transitions from 0 to 1 or vice versa when the binary string is considered circularly. For P neighboring pixels, $\mathrm{LBP}^{u2}_{P,R}$ lead to a histogram of $P \times (P - 1) + 3$ dimensions. When "uniform patterns" codes are rotated to their minimum values, denoted by $\mathrm{LBP}^{\mathrm{riu2}}_{P,R}$ [23], the total number of patterns reduces to $P + 2$:

$$\mathrm{LBP}^{\mathrm{riu2}}_{P,R} = \begin{cases} \sum_{n=0}^{P-1} s(g_n - g_c), & U(\mathrm{LBP}_{P,R}) \leq 2, \\ P + 1, & \text{Otherwise}, \end{cases} \tag{8}$$

where the U value of an LBP pattern is defined as the number of spatial transitions (bitwise 0 and 1 changes) in that pattern. Therefore,

$$U(\mathrm{LBP}_{P,R}) = \left|s(g_{P-1} - g_c) - s(g_0 - g_c)\right| + \sum_{n=1}^{P-1} \left|s(g_n - g_c) - s(g_{n-1} - g_c)\right|. \tag{9}$$

4. The Proposed Method

In this section, the proposed method for region duplication image forgery based on Harris feature points and local binary patterns is described in detail. The flow diagram of our algorithm is shown in Figure 3. The whole detection steps are given as follows.

Step 1 (preprocessing the input image). In our algorithm, we are concerned with gray level images. For a color image in RGB model, it is first converted to a grayscale image using the standard formula

$$Y = 0.299R + 0.587G + 0.114B, \tag{10}$$

where R, G, and B are three channels of the input color image and Y is its luminance component.

As mentioned before, several image postprocessing operations could be involved in practical region duplication forgery, such as noise adding, JPEG compression, or blurring. It is well known that the high frequency components are not stable when the image is distorted by these postprocessing operations, while the low frequency features are more resistant to these distortions. Thus, in the preprocessing stage, we filter the input image with a pixelwise adaptive Wiener method based on statistics estimated from a local neighborhood of each pixel. With lots of experiments, we find that this filtering in the preprocessing stage has significant improvements on detection performance. Besides, extensive experiments show that multiple filtering contributes to the improvements, especially when the input image is suffering from severe AWGN and JPEG compression. In our experiments, we find that for high strength JPEG compression or AWGN with low SNR five times of filtering is an optimal option. However, for moderate distortions one time of filtering is in effect.

Step 2 (Harris feature points detection and feature extraction). Harris feature points in the filtered image are detected. As described in Section 3.1, dense Harris feature points are employed in order to obtain a sufficient number of feature points with approximately uniform distribution. After obtaining location coordinates of each feature point, LBP is applied to each pixel in a circle patch with the radius of 10 around each feature point. In the proposed algorithm, by means of using rotation invariant uniform LBP ($\mathrm{LBP}_{P,R}^{\mathrm{riu2}}$) and various combinations of P/R values, we can realize operators for any quantization of angular space and for any spatial resolution, which combine the information provided by multiple LBP operators.

In our experiments, three variants of rotation invariant uniform LBP, including $\mathrm{LBP}_{8,1}^{\mathrm{riu2}}$, $\mathrm{LBP}_{12,2}^{\mathrm{riu2}}$, and $\mathrm{LBP}_{16,2}^{\mathrm{riu2}}$, are applied to the circle patch around each feature point to extract the features. For a given circle patch with the radius of 10 around the nth feature point, three histograms of rotation invariant uniform LBP, denoted by $V_{1,n}(\mathrm{LBP}_{8,1}^{\mathrm{riu2}})$, $V_{2,n}(\mathrm{LBP}_{12,2}^{\mathrm{riu2}})$, and $V_{3,n}(\mathrm{LBP}_{16,2}^{\mathrm{riu2}})$, are used as feature vectors, which are computed using $\mathrm{LBP}_{8,1}^{\mathrm{riu2}}$, $\mathrm{LBP}_{12,2}^{\mathrm{riu2}}$, and $\mathrm{LBP}_{16,2}^{\mathrm{riu2}}$, respectively. It should be noticed that each feature vector is normalized to unit length. Extracted feature vectors are put in separate feature matrices. Assuming that the total number of Harris feature points is N, thus we can obtain three feature matrices of size $N\times(P+2)$, to be specific, FM_1, FM_2, and FM_3, with dimensions of $N \times 10$, $N \times 14$, and $N \times 18$, respectively.

Step 3 (feature matching). In the feature matching step, the similar Harris points are matched based on their representation feature vectors using the best-bin-first (BBF) algorithm [25] to determine the duplicated regions correctly. For a Harris feature point at location $\mathbf{x}$ with feature vector $\mathbf{f}$, we match it with point at location $\widetilde{\mathbf{x}}$, whose corresponding feature vector $\widetilde{\mathbf{f}}$ is the nearest neighbor to $\mathbf{f}$ measured with L_2 (Euclidean) distance. It is well known that due to the smoothness of natural image, the best match of a feature point usually lies within its close spatial adjacency. Thus, in order to avoid searching nearest neighbors of a feature point from the same region, we perform the search outside a 10×10 pixels circle window centered at the feature point. Only pair-wise points with distinct similarities are kept in the matching step. Specifically, we require that, for any other feature vector $\mathbf{f}^*$ other than $\mathbf{f}$ and $\widetilde{\mathbf{f}}$, the L_2 distance between $\mathbf{f}$ and $\widetilde{\mathbf{f}}$ has to be smaller than that between $\mathbf{f}$ and $\mathbf{f}^*$ by at least a threshold T:

$$\frac{\left\|\widetilde{\mathbf{f}}-\mathbf{f}\right\|_2}{\left\|\mathbf{f}^*-\mathbf{f}\right\|_2} < T, \tag{11}$$

where $T \in (0,1)$ is a preset threshold controlling the distinctiveness of feature matching.

For each feature matrix of FM_1, FM_2, and FM_3, we record the indexes of every pair-wise matching points satisfying (11). Formally, let $(P\,\mathrm{index}_1, P\,\mathrm{index}_2)$ be an index pair of the two feature points which are represented by two rows of each feature matrix. Due to the order of an index pair making no difference, the index pair of matching points is normalized, if necessary, by interchange of positions so that $P\,\mathrm{index}_1 \le P\,\mathrm{index}_2$. For each index pair $(P\,\mathrm{index}_1, P\,\mathrm{index}_2)$, we increment a matching frequency counter C by one as follows:

$$C\left(P\,\mathrm{index}_1, P\,\mathrm{index}_2\right) = C\left(P\,\mathrm{index}_1, P\,\mathrm{index}_2\right) + 1. \tag{12}$$

The matching frequency counter C is initialized to zero before the algorithm starts. At the end of the matching process, the counter C indicates the frequencies with which different index pairs of matching points, which are determined by three feature matrices FM_1, FM_2, and FM_3, respectively, occur. To determine the candidate matching points, the majority rule is utilized. Specifically, all the pair-wise matching points are found, whose occurrence exceeds twice. The matching strategy of feature points is applied for all Harris feature points in the corresponding matrices FM_1, FM_2, and FM_3, and final matching results are stored in a similar points matrix SPM, which records the corresponding spacial coordinates of matching points.

Step 4 (removing false matches and outputting detection result map). Due to a portion of mismatched feature points, we employ a widely used robust estimation method known as the Random Sample Consensus (RANSAC) algorithm [26] to remove false matches in the similar points matrix SPM. The final detection result map is output with color lines connecting all the matching points to identify the duplicated region and forgery region.

5. Experimental Results and Analysis

In our experiments, the tampered images were created by Adobe Photoshop CS3 based on the following two datasets. The first one contains 24 uncompressed PNG true color images with the size of 768×512 pixels released by Kodak Corporation for unrestricted research usage [27]. In addition, we collected 50 high resolution color images of size 1024×768 pixels from Google image search [28], which formed the second dataset. Through a large number of repeated experiments, threshold T is fixed to 0.5, and the size of Wiener filter window is set to [5 5]. All the experiments were carried out on the platform with Intel Pentium 2.13 GHz and MATLAB R2010b. By using our method, for each image with the two different sizes from the two datasets mentioned above, it takes about 9 s and 13 s to locate the tampered regions, respectively, which are of high efficiency. Nevertheless, if we use C++ or Java programming languages to implement the algorithm, our algorithm will achieve higher efficiency.

5.1. Performance Evaluation. For practical applications, the most important aspect of a detection method is the ability to distinguish tampered and original images. Thus we adopt the evaluation indexes which are defined in [17] to evaluate the performance of our algorithm at image level. We keep a record of some important measures including the number of correctly detected forged images T_P, the number of images that have been erroneously detected as forged F_P, and

(a) Hiding specific objects

(b) Adding specific objects/multiple region duplication forgery

(c) Hiding specific objects/homogenous background forgery

Figure 4: Shown are the detection results of nonregular region duplication forgeries without any postprocessing operations.

the falsely missed forged images F_N. From these we can obtain two evaluation indexes precision, p, and recall, r, as follows:

$$p = \frac{T_P}{T_P + F_P}, \qquad r = \frac{T_P}{T_P + F_N}. \tag{13}$$

Precision denotes the probability that a detected forgery is truly a forgery, while recall shows the probability that a forged image is detected.

5.2. Effectiveness Test. In the following experiment, we select some original images from the two datasets above-mentioned to test the effectiveness of our algorithm. It is noted that all the duplicated regions are nonregular and meaningful objects, which are commonly true in realistic tampered images with high resolution. All the doctored images in this experiment are without any postprocessing operation and the corresponding detection results are illustrated in Figure 4. The first column shows the original images, the second one gives the tampered images, and the third one shows the detection results. Owing to space constraints, just a part of the experimental results is given here. Figure 4(a) illustrates the case of hiding specific objects and Figure 4(b) shows the case of adding specific objects, which indicates that our algorithm can expose regions of duplication forgeries effectively. Images shown in Figure 4(b) also demonstrate that our algorithm works well even when the tampered images have multiple duplicated regions. The doctored image in Figure 4(c) shows the specific scenario that there are large similar or flat regions in the image, such as large areas of water, sky or grass. Due to the homogenous background in the suspicious images, it is, challenge to discern the forgery. To the best of our knowledge, a number of existing methods cease to be effective under the circumstances; however, the detection results of our algorithm are satisfactory. It is noted that the proposed method outputs detection result maps with color lines connecting all the matching points to identify the duplicated region and forgery region. Although the forgery region cannot be localized precisely to pixel level, we can easily identify the tampered region by color lines, which is sufficient for practical detection requirements.

5.3. Robustness Test. Since forgers usually do their utmost to create an imperceptible tampered image, various kinds of intermediate operations and postprocessing operations are carried out such as rotation, flipping, additive Gaussian noise, Gaussian blurring, JPEG compression, or their mixed operations. In this section, we conduct a series of experiments

(a) Rotation 15 degrees

(b) Rotation 180 degrees

(c) Rotation 270 degrees

(d) Horizontal flipping

(e) Vertical flipping

Figure 5: Shown are the detection results of nonregular region duplication forgeries with intermediate operations rotation and flipping.

to test the robustness of the proposed method. Figure 5 indicates that our algorithm can identify duplicated regions in the cases of different angles of rotation and horizontal and vertical flipping with a satisfactory degree. Images shown in Figure 6 illustrate that the proposed algorithm can effectively locate the duplicated regions under common postprocessing operation including Gaussian blurring, AWGN, and JPEG compression, even when the quality of distorted image is pretty poor, such as Gaussian blurring ($w = 7$, $\sigma = 5$), AWGN (SNR = 10 dB), and JPEG compression ($Q = 20$).

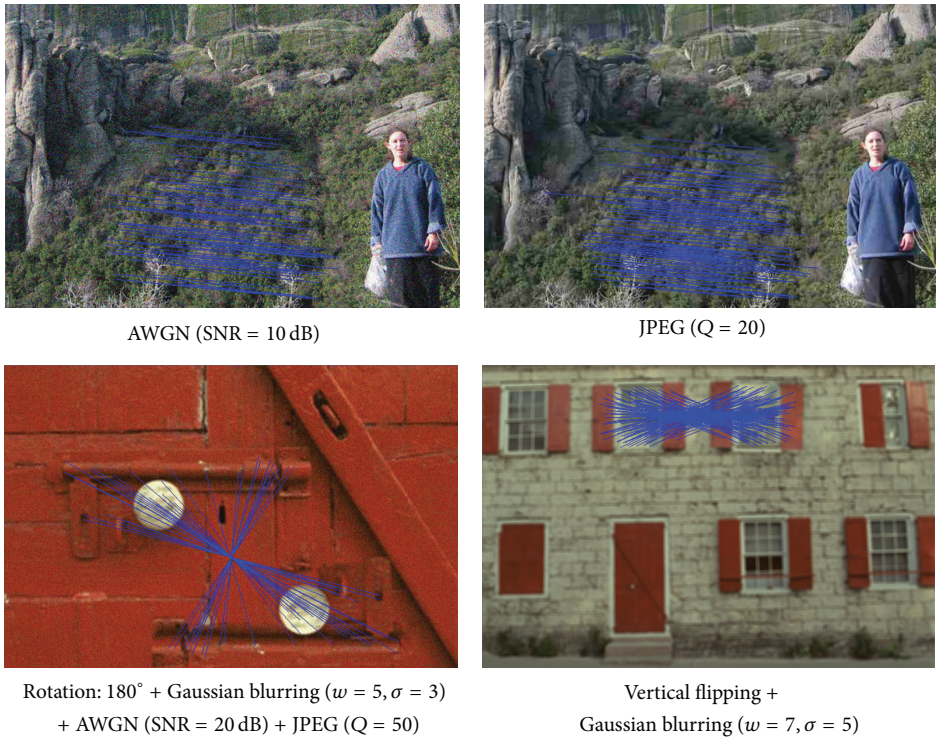


Figure 6: Shown are the detection results of nonregular region duplication forgeries under different postprocessing operations.

It is particularly worth mentioning that our method is robust, even when tampered images are distorted by mixed operations of rotation/flipping transformations and postprocessing operations.

Furthermore, in order to evaluate quantitatively the robustness of our algorithm to different image distortions, we selected randomly 50 original images from the two datasets to generate forged images by copying a square region at a random location and pasting it onto a nonoverlapping region. The sizes of square region were 60×60 pixels, 80×80 pixels, and 100×100 pixels, respectively, each kind of which included translating and two different intermediate operations to generate 450 tampered images. The intermediate operations were flipping (horizontal and vertical) and rotation (90/180/270 degrees), respectively. These tampered images were then distorted by commonly used postprocessing operations with different parameters, such as Gaussian blurring, AWGN, and JPEG compression. In order to obtain more credible evaluation indexes, 300 authentic images from CASIA V2.0 [29] were chosen randomly together with 50 original images and all the distorted images to compose a robustness testing image set. The experimental results were given in Figure 7. In general, the detection results shown in Figure 7 indicate that the larger the area of duplicated region is, the better the detection performance would be, no matter which post-operation the image is distorted by. As can be seen from Figure 7(a), the proposed method has a high detection performance when the images are distorted by Gaussian blurring, even when the image has poor quality ($w = 7$, $\sigma = 4$) and small forgery region (60×60 pixels), where the precision rate is larger than 89% and the recall rate is larger than 80% in all the cases with different parameters of Gaussian blurring filter. We can draw a conclusion from Figure 7(b) that our method performs well also in the case of processing AWGN distorted images. The precision rate is over 80% till SNR drops to 15 dB, even though there is a slight decay in the recall rate when SNR drops. Results of tampered images distorted by JPEG compression with different quality are shown in Figure 7(c), which indicate that our method performs well in the case of JPEG compression.

5.4. Comparison of Detection Performance. In the last experiment, we compared our method with the method in [11], a typical keypoint-based scheme, based on the SIFT keypoints detection and feature matching which is robust to rotation, scaling, and some postprocessing operations including AWGN and JPEG compression. In [11], the duplicated region is required to contain more than 50 SIFT keypoints, however, which is unrealistic in many practical detections since the duplicated region may not guarantee so many SIFT keypoints especially when the copied region exhibits little structure. Further, according to our experiments, the SIFT method [11] is sensitive to blurring artifacts and if the copied region exhibits little structure or small forgery area, it may happen that the region is completely missed [17].

In contrast to the popular keypoint-based scheme based on SIFT keypoints detection in [11, 12], the proposed method has good robustness against flipping artifacts and Gaussian blurring. As mentioned before, the method in [11, 12] is only possible to extract the keypoints from peculiar points of

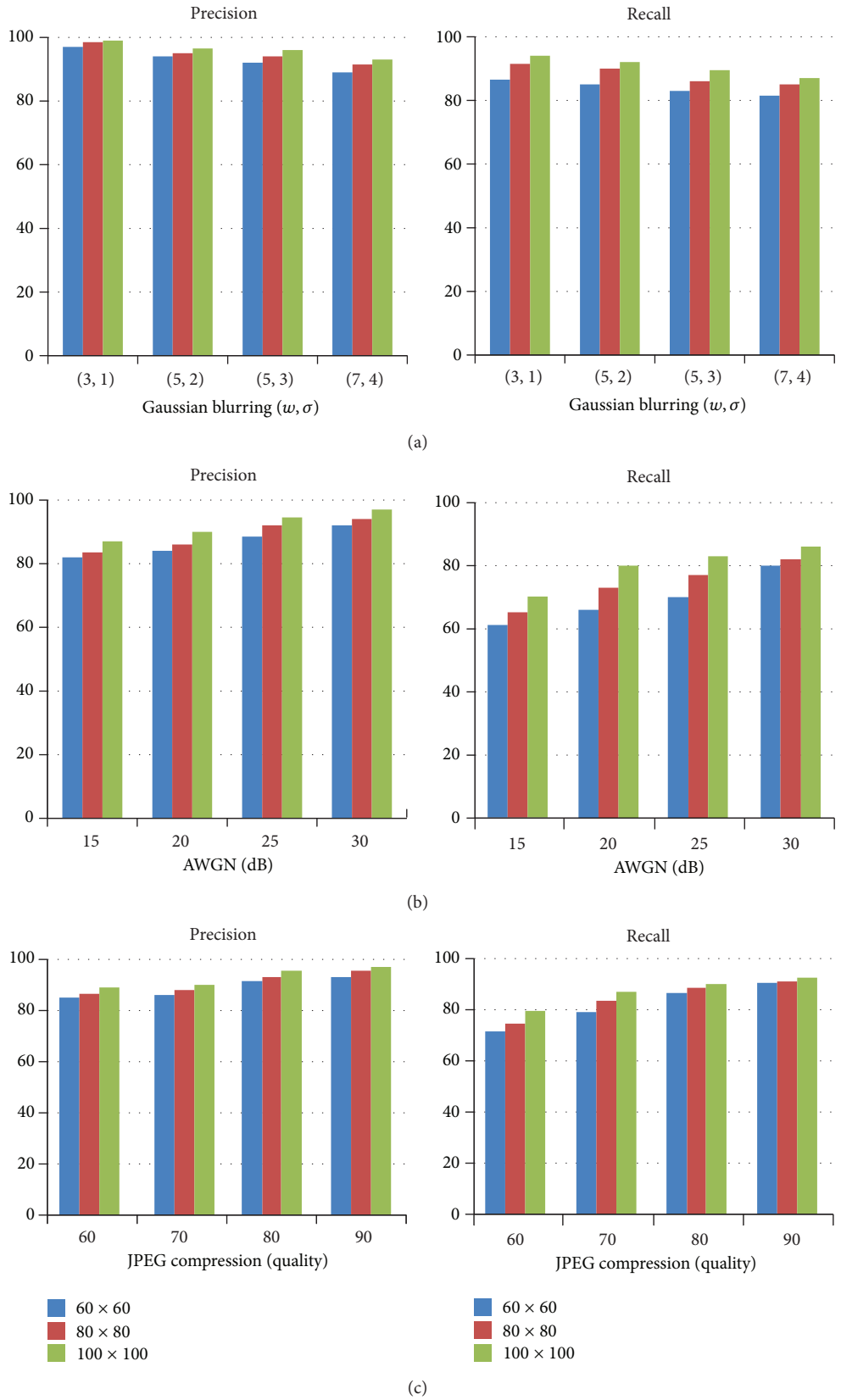
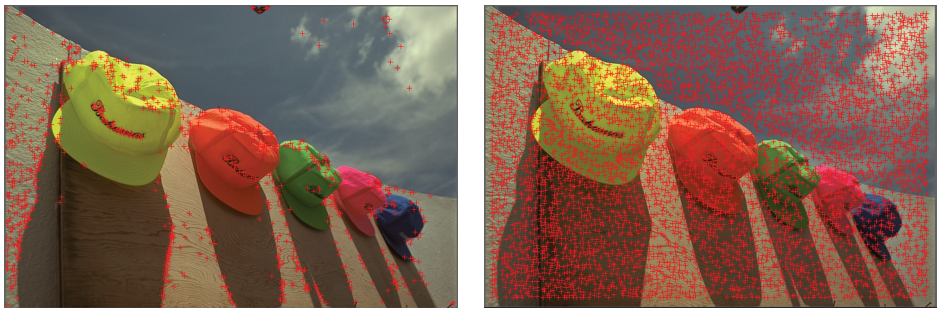


Figure 7: Shown are comparisons of average detection performance of the proposed method. Precision and recall in (a) Gaussian blurring, (b) AWGN, and (c) JPEG compression.



(a) SIFT points-987 (b) Dense Harris points-5175

Figure 8: Comparison of the number and distribution of different feature points.

Figure 9: Shown is the detection result of region duplication forgery with little visual structures.

the image and not robust to some postprocessing operations like blurring and flipping based on our experimental results. Moreover, if the copied region exhibits little visual structure or small area, it may happen that the region is completely missed. However, our method performs well in this kind of scenario. The main reason is that our method employs the dense Harris feature points which is superior to SIFT feature points in [11, 12]. Figure 8 gives an example of different feature detection methods in the same image that shows the number and distribution situation of feature points. As seen in Figure 8, there are 987 feature points detected by SIFT algorithm, while 5175 dense Harris feature points are detected by our method. What is more, the distribution of feature points is widely divergent. As shown in Figure 8(a), SIFT algorithm cannot find reliable feature points in regions with little visual structures, and it is also hard to detect in smaller regions. However, dense Harris feature points employed in our method are nearly well distributed in the image shown in Figure 8(b). Consequently, our method can effectively detect the forgery regions with little visual structures, such as large areas of sky, grass, or water. One example is shown in Figure 9, where an obvious duplicated region is not detected by the SIFT method [11, 12] since SIFT algorithm cannot find reliable feature points in the forgery region. The detection result using our method is shown in the third column of Figure 9, which demonstrates that the proposed method can effectively detect the forgery region with little visual structures.

In the last experiment, we compared our method with two typical approaches: FMT-based [8] and SIFT-based [11], which belong to block-based and keypoint-based detection methods, respectively. Here we still randomly selected 50 original images from the two datasets to generate forged images by copying a square region at a random location and pasting it onto a nonoverlapping region. The sizes of square region were 60×60 pixels, 80×80 pixels, and 100×100 pixels, respectively and included three differently relative locations to generate 450 tampered images. In the first scenario, we evaluated the three algorithms in the case of rotation duplication forgery, where the duplicate region was copied and then rotated with a random angle $\theta \in \{0^\circ, 2^\circ, 5^\circ, 10^\circ, 15^\circ, 90^\circ, 180^\circ, 270^\circ\}$ before pasting. In the second scenario, horizontal and vertical flipping were considered. In the third scenario, these tampered images were distorted by commonly used postprocessing operations with a random parameter just as Section 5.3 showed, including Gaussian blurring, AWGN, and JPEG compression. All the distorted images in the above-mentioned three cases together with their original version and 300 authentic images from CASIA V2.0 composed three test image sets, respectively. The corresponding experimental results are shown in Figure 10. As can be seen from Figure 10, compared to the SIFT-based [11] and FMT-based [8], the proposed method has a high detection performance when the images are distorted by Gaussian blurring, AWGN, and JPEG compression. There are two main reasons for this. On one hand, we first filter the input image with a pixelwise adaptive Wiener method based on statistics estimated from a local neighborhood of each pixel, which has significant improvements on detection performance, especially when the input image is suffering from severe AWGN and JPEG compression. On the other hand, among those doctored images that are not detected by the SIFT method [11], most of them are due to lacking reliable SIFT keypoints in the duplicated region with little visual structures. According to Figure 10, we can also see that

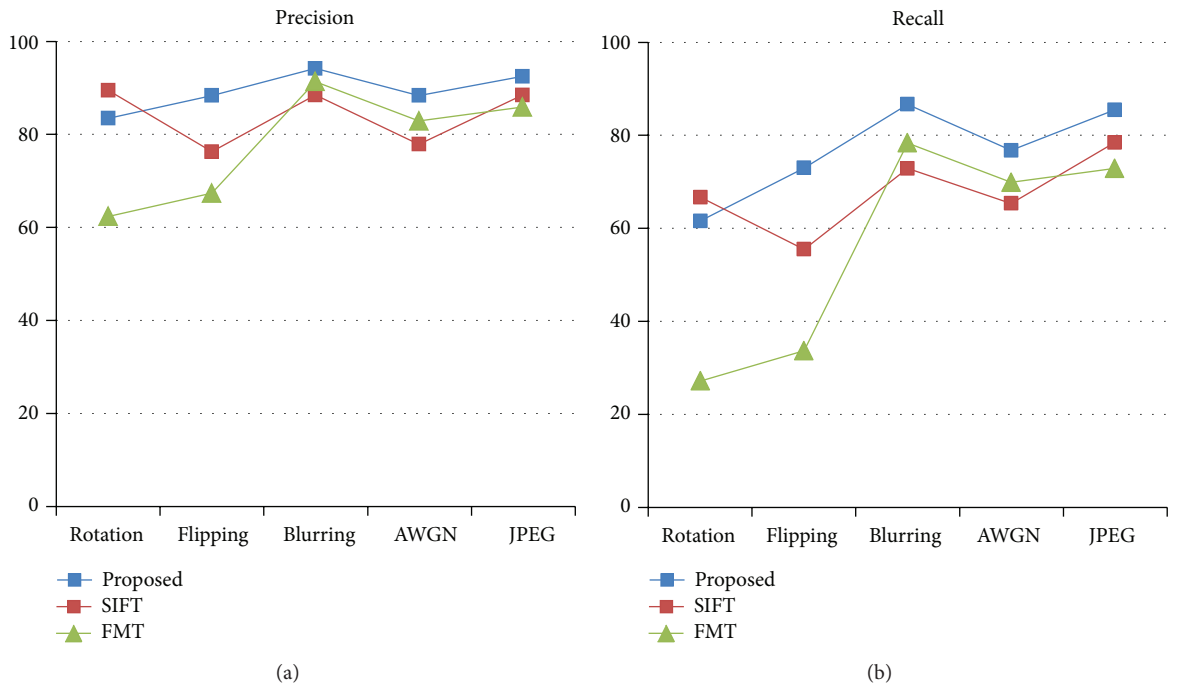


Figure 10: Shown is a comparison of detection performances of FMT, SIFT, and proposed methods.

the proposed method has a comparative advantage for the detection of flipping forgery, while the SIFT method [11] is slightly superior to the proposed method in terms of rotation detection. The main reason would be that the detection performance of proposed method is slightly inferior to that of the SIFT method [11] in the rotation angles without a multiple of 90° degrees (90°, 180°, 270°, and 360°).

6. Conclusion

In this paper a passive forensic method based on Harris feature points and local binary patterns for detecting region duplication image forgery is proposed. We demonstrate the effectiveness of our detection method with a series of experiments on lots of realistic forgery images with high resolution. Experimental results show that the proposed method can effectively detect region duplication forgery, even when an image was distorted by rotation, flipping, blurring, AWGN, JPEG compression, and their mixed operations, especially resistant to the forgery with the flat area of little visual structures. Although having achieved promising detection performance, the proposed method fails to detect region duplication forgery with scaling on account of the fact that Harris corners and LBP are sensitive to image scaling not being computed on multiscale image layers, which is an important work in our future study.

Conflict of Interests

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

Acknowledgment

This work was supported by Higher School Science & Technology Fund Planning Project of Tianjin City (no. 20120712), China.

References

[1] A. Mishra, A. Goel, R. Singh, G. Chetty, and L. Singh, "A novel image watermarking scheme using extreme learning machine," in *Proceedings of the International Joint Conference on Neural Networks (IJCNN '12)*, pp. 1–6, 2012.

[2] X. Tong, Y. Liu, M. Zhang, and Y. Chen, "A novel chaos-based fragile watermarking for image tampering detection and self-recovery," *Signal Processing*, vol. 28, pp. 301–308, 2013.

[3] L. Weiqi, H. Jiwu, and Q. Guoping, "Robust detection of region-duplication forgery in digital image," in *Proceedings of the 18th International Conference on Pattern Recognition (ICPR '06)*, pp. 746–749, August 2006.

[4] J. Fridrich, D. Soukalm, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, pp. 55–61, Cleveland, Ohio, USA, 2003.

[5] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Dartmouth College, 2004.

[6] K. Xiaobing and W. Shengmin, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proceedings of the International Conference on Computer Science and Software Engineering (CSSE '08)*, pp. 926–930, December 2008.

[7] L. Guohui, W. Qiong, T. Dan, and S. Shaojie, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *Proceedings of*

the IEEE International Conference on Multimedia and Expo (ICME '07), pp. 1750–1753, July 2007.

[8] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 1053–1056, IEEE Press, New York, NY, USA, April 2009.

[9] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic Science International*, vol. 206, no. 1–3, pp. 178–184, 2011.

[10] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," *Forensic Science International*, vol. 214, no. 1–3, pp. 33–43, 2012.

[11] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 857–867, 2010.

[12] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[13] H. Hailing, G. Weiqiang, and Z. Yu, "Detection of copy-move forgery in digital images using sift algorithm," in *Proceedings of the Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA '08)*, pp. 272–276, December 2008.

[14] B. Xu, J. Wang, G. Liu, and Y. Dai, "Image copy-move forgery detection based on SURF," in *Proceedings of the 2nd International Conference on Multimedia Information Networking and Security (MINES '10)*, pp. 889–892, November 2010.

[15] B. L. Shivakumar and S. Baboo, "Detection of region duplication forgery in digital images using SURF," *International Journal of Computer Science Issues*, vol. 8, no. 4, pp. 199–205, 2011.

[16] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics," *Signal Processing*, vol. 91, no. 8, pp. 1759–1770, 2011.

[17] V. Christlein, C. Riess, J. Jordan et al., "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[18] C. Harris and M. Stephens, "A combined corner and edge detector," in *Proceedings of the Alvey Vision Conference*, pp. 147–151, The Plessey Company Pic, Vicarage Lane, UK, 1988.

[19] Y. Yang, G. Cheng, and D. Tu, "An image quality metric based on the Harris corner," in *Proceedings of the International Conference on Signal Processing (ICSP '12)*, pp. 873–876, 2012.

[20] J. Yang, S. Wang, and X. Du, "Remote sensing image matching algorithm based on Harris and SIFT transform," *Journal of Theoretical and Applied Information Technology*, vol. 46, no. 1, pp. 333–338, 2012.

[21] T. Chang, F. Yu, W. Lee et al., "Free view point real-time monitor system based on Harris-SURF. Smart innovation," *System and Technologies*, no. 21, pp. 423–430, 2013.

[22] H. Zhang, X. Chen, X. Gao et al., "An indoor mobile visual localization algorithm based on Harris-SIFT," *Intelligent Automation and Soft Computing*, vol. 12, no. 7, pp. 885–897, 2012.

[23] T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, 2002.

[24] C. Zhu, C. Bichot, and L. Chen, "Image region description using orthogonal combination of local binary patterns enhanced with color information," *Pattern Recognition*, no. 46, pp. 1949–1963, 2013.

[25] J. S. Beis and D. G. Lowe, "Shape indexing using approximate nearest-neighbour search in high-dimensional spaces," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 1000–1006, June 1997.

[26] M. A. Fischler and R. C. Bolles, "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," *Communications of the ACM*, vol. 24, no. 6, pp. 381–395, 1981.

[27] "Kodak Lossless True Color Image Suite," http://r0k.us/graphics/kodak.

[28] "Google Image Search," http://images.google.com.

[29] "CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v2.0)," http://forensics.idealtest.org.