This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



# Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching

Chi-Man Pun, *Senior Member, IEEE*, Xiao-Chen Yuan, *Member, IEEE,* and Xiu-Li Bi[1]

***Abstract*—A novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching is proposed in this paper. The proposed scheme integrates both block-based and keypoint-based forgery detection methods. First, the proposed Adaptive Over-Segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the Forgery Region Extraction algorithm, which replaces the feature points with small superpixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions; finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy-move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy-move forgery detection methods.**

***Index Terms*—Copy-Move Forgery Detection, Adaptive Over-Segmentation, Local Color Feature, Forgery Region Extraction**

## I. Introduction

With the development of computer technology and image processing software, digital image forgery has been increasingly easy to perform. However, digital images are a popular source of information, and the reliability of digital images is thus becoming an important issue. In recent years, more and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery [1], which is to paste one or several copied region(s) of an image into other part(s) of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case. In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms [1-13] and feature keypoint-based algorithms [14-19].

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Fridrich et al. [1] proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. Popescu and Farid [2] applied Principal Component Analysis (PCA) to reduce the feature dimensions. Luo et al. [3] used the RGB color components and direction information as block features. Li et al. [4] used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic [5] calculated the 24 Blur-invariant moments as features. Kang and Wei [6] calculated the singular values of a reduced-rank approximation in each block. Bayram et al. [7] used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. [8, 9] used the mean intensities of circles with different radii around the block center to represent the block features. Lin et al. [10] used the gray average results of each block and its sub-blocks as the block features. Ryu et al. [11, 12] used Zernike moments as block features. Bravo-Solorio and Nandi [13] used information entropy as block features.

As an alternative to the block-based methods, keypoint-based forgery detection methods were proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In [14-16, 18], the Scale-Invariant Feature Transform (SIFT) [20] was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector


This research was supported in part by the Research Committee of the University of Macau (MYRG181-FST11-PCM, MYRG2015-00012-FST, MYRG2015-00013-FST) and the Science and Technology Development Fund of Macau SAR (FDCT 008/2013/A1, FDCT 093-2014-A2).

[1] Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi are with Department of Computer and Information Science, University of Macau, Macau SAR, China. E-mail: {cmpun, xcyuan, yb47429}@umac.mo

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In [17, 19], the Speeded Up Robust Features (SURF) [21] were applied to extract features instead of SIFT. However, although these methods can locate the matched keypoints, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate [22].

Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Although these algorithms are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases; 2) the methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Although the existing keypoint-based forgery detection methods can avoid the first two problems, they can reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing keypoint-based forgery methods were very poor.

To address the above-mentioned problems, in this paper, we propose a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching. The proposed scheme integrates both the traditional block-based forgery detection methods and keypoint-based forgery detection methods. Similar to block-based forgery detection methods, we propose an image-blocking method called the Adaptive Over-Segmentation algorithm to divide the host image into non-overlapping and irregular blocks adaptively. Then, similar to the keypoint-based forgery detection methods, the feature points are extracted from each image block as block features instead of being extracted from the whole host image as in the traditional keypoint-base methods. Subsequently, the block features are matched with one another to locate the labeled feature points, which can approximately indicate the suspected forgery regions. To detect more accurate forgery regions, we proposed the Forgery Region Extraction algorithm, which replaces the feature points with small superpixels as feature blocks and, then, merges the neighboring blocks with similar local color features into feature blocks, to generate the merged regions; finally, it applies a morphological operation into the merged regions to generate the detected forgery regions.

In the following sections, Section II shows the framework of the proposed copy-move forgery detection scheme and then explains each step in detail. In section III, a series of experiments are conducted to demonstrate the effectiveness of our proposed scheme. Finally, the conclusions are drawn in section IV.

## II. Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching

This section describes the proposed image forgery detection using adaptive over-segmentation and feature point matching in detail. Fig. 1 shows the framework of the proposed image forgery detection scheme. First, an adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks called Image Blocks (IB). Then, we apply the Scale Invariant Feature Transform (SIFT) in each block to extract the SIFT feature points as Block Features (BF). Subsequently, the block features are matched with one another, and the feature points that are successfully matched to one another are determined to be Labeled Feature Points (LFP), which can approximately indicate the suspected forgery regions. Finally, we propose the Forgery Region Extraction method to detect the forgery region from the host image according to the extracted LFP. In the remainder of this section, Section II-A explains the proposed Adaptive Over-Segmentation method in detail; Section II-B introduces the Feature Point Extraction using SIFT; Section II-C describes the Block Feature Matching procedures; and Section II-D presents the proposed Forgery Region Extraction method.

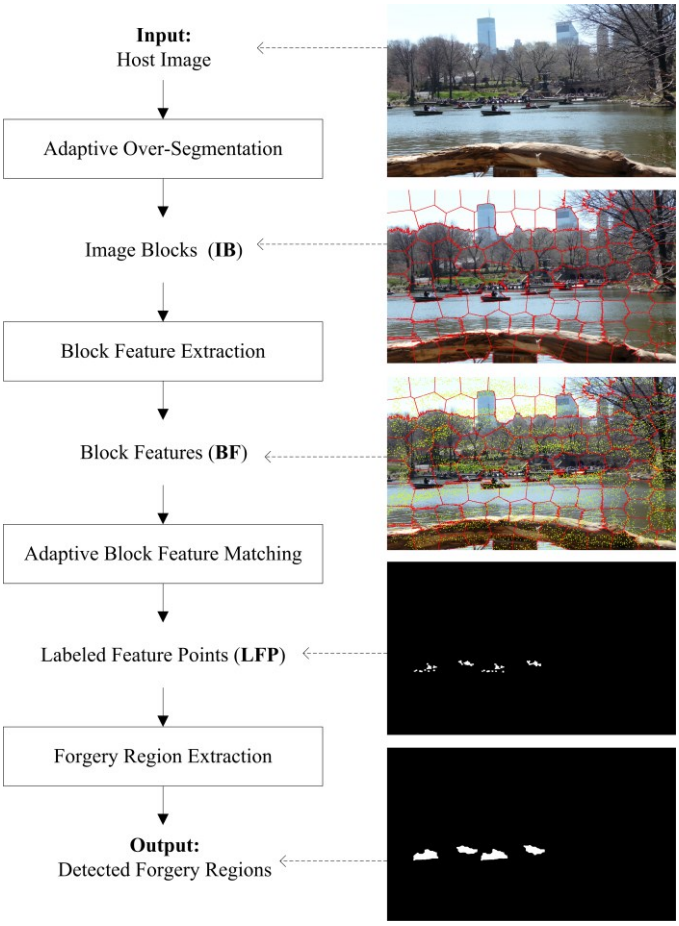


Fig. 1 Framework of the proposed copy-move forgery detection scheme

### A. Adaptive Over-Segmentation Algorithm

In our copy-move forgery detection scheme, we first propose the Adaptive Over-Segmentation algorithm, which is similar to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



the traditional block-based forgery detection methods and can divide the host image into blocks. In previous years, a large amount of block-based forgery detection algorithms have been proposed [1-13]. Of the existing block-based forgery detection schemes, the host image was usually divided into overlapping regular blocks, with the block size being defined and fixed beforehand, as shown in Fig. 2-(a) and (b). Then, the forgery regions were detected by matching those blocks. In this way, the detected regions are always composed of regular blocks, which cannot represent the accurate forgery region well; as a consequence, the recall rate of the block-based methods is always very low, for example, as in [8, 9]. Moreover, when the size of the host images increases, the matching computation of the overlapping blocks will be much more expensive. To address these problems, we proposed the Adaptive Over-segmentation method, which can segment the host image into non-overlapping regions of irregular shape as image blocks, as shown in Fig. 2-(c); afterward, the forgery regions can be detected by matching those non-overlapping and irregular regions.

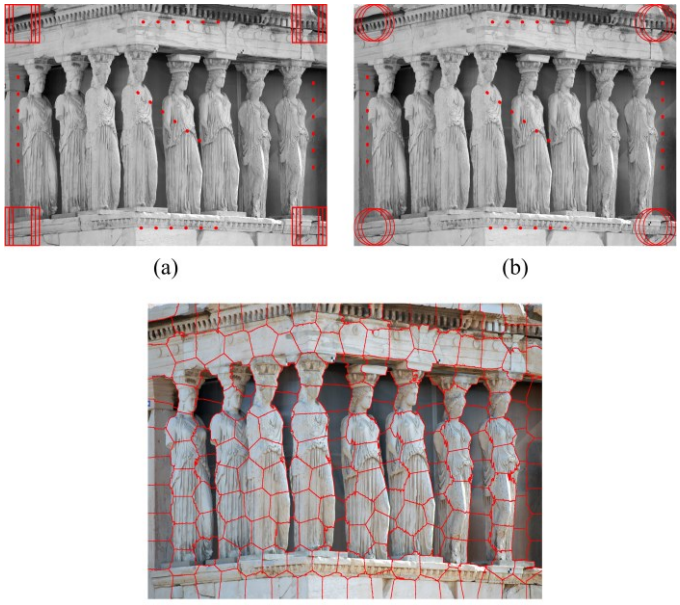

Fig. 2 Different blocking / segmentation methods (a) Overlapping and rectangular blocking; (b) Overlapping and circular blocking; and (c) Non-overlapping and irregular blocking.

Because we must divide the host image into non-overlapping regions of irregular shape and because the superpixels are perceptually meaningful atomic regions that can be obtained by over-segmentation, we employed the simple linear iterative clustering (SLIC) algorithm [23] to segment the host image into meaningful irregular superpixels, as individual blocks. The SLIC algorithm adapts a k-means clustering approach to efficiently generate the superpixels, and it adheres to the boundaries very well. Fig. 2 shows the different blocking / segmentation methods, where (a) shows the overlapping and rectangular blocking, (b) shows the overlapping and circular blocking, and (c) shows the non-overlapping and irregular blocking with the SLIC segmentation method. Using the SLIC segmentation method, the non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocking; furthermore, in most cases, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the superpixels in SLIC is difficult to decide.

In practical applications of copy-move forgery detection, the host images and the copy-move regions are of different sizes and have different content, and in our forgery detection method, different initial sizes of the superpixels can produce different forgery detection results; consequently, different host images should be blocked into superpixels of different initial sizes, which is highly related to the forgery detection results. In general, when the initial size of the superpixels is too small, the result will be a large computational expense; otherwise, when it is too large, the result will be that the forgery detection results are not sufficiently accurate. Therefore, a balance between the computational expense and the detection accuracy must be obtained when employing the SLIC segmentation method for image blocking.

In general, the proper initial size of the superpixels is very important to obtain good forgery detection results for different types of forgery regions. However, currently, there is no good solution to determine the initial size of the superpixels in the existing over-segmentation algorithms. In this paper, we propose a novel Adaptive Over-Segmentation method that can determine the initial size of the superpixels adaptively based on the texture of the host image. When the texture of the host image is smooth, the initial size of the superpixels can be set to be relatively large, which can ensure not only that the superpixels can get close to the edges but also that the superpixels will contain sufficient feature points to be used for forgery detection; furthermore, larger superpixels imply a smaller number of blocks, which can reduce the computational expense when the blocks are matched with one another. In contrast, when the texture of the host image has more detail, then the initial size of the superpixels can be set to be relatively small, to ensure good forgery detection results. In the proposed method, the Discrete Wavelet Transform (DWT) is employed to analyze the frequency distribution of the host image. Roughly, when the low-frequency energy accounts for the majority of the frequency energy, the host image will appear to be a smooth image; otherwise, if the low-frequency energy accounts for only a minority of the frequency energy, the host image appears to be a detailed image.

We have performed a large number of experiments to seek the relationship between the frequency distribution of the host images and the initial size of the superpixels to obtain good forgery detection results. We performed a four-level DWT, using the 'Haar' wavelet, on the host image; then, the low-frequency energy $E_{LF}$ and high-frequency energy $E_{HF}$ can be calculated using (1) and (2), respectively. With the low-frequency energy $E_{LF}$ and high-frequency energy $E_{HF}$, we can calculate the percentage of the low-frequency distribution $P_{LF}$ using (3), according to which the initial size $S$ of the superpixels can be defined as in (4).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



$$E_{LF} = \sum |CA_4| \quad (1)$$

$$E_{HF} = \sum_i (\sum |CD_i| + \sum |CH_i| + \sum |CV_i|), i = 1,2,...,4 \quad (2)$$

where $CA_4$ indicates the approximation coefficients at the 4th level of DWT; and $CD_i$, $CH_i$ and $CV_i$ indicate the detailed coefficients at the $i^{th}$ level of DWT, $i = 1,2,...,4$.

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}} \cdot 100\% \quad (3)$$

$$S = \begin{cases} \sqrt{0.02 \times M \times N} & P_{LF} > 50\% \\ \sqrt{0.01 \times M \times N} & P_{LF} \le 50\% \end{cases} \quad (4)$$

where $S$ means the initial size of the superpixels; $M \times N$ indicates the size of the host image; and $P_{LF}$ means the percentage of the low-frequency distribution.

In summary, the flow chart of the proposed Adaptive Over-Segmentation method is shown in Fig. 3. First, we employed the DWT to the host image to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, we calculated the percentage of the low-frequency distribution $P_{LF}$ using (3), according to which we determined the initial size *S*, using (4). Finally, we employed the SLIC segmentation algorithm together with the calculated initial size *S* to segment the host image to obtain the image blocks (IB).

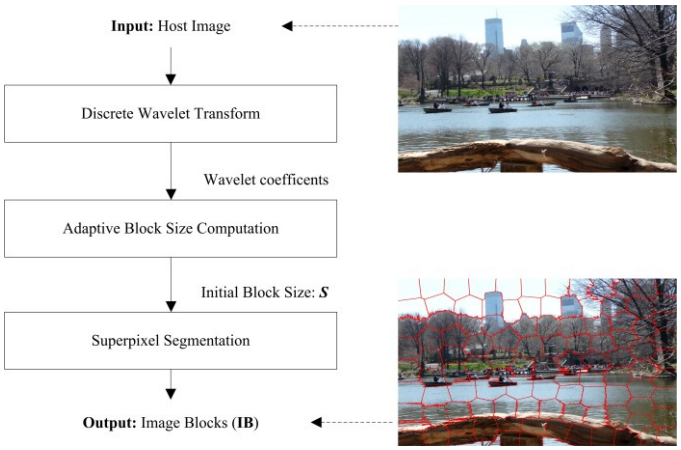


Fig. 3 Flowchart of the Adaptive Over-Segmentation algorithm

Using the Adaptive Over-Segmentation method described above, in Fig. 4-(A1), the size of the host image I1 is $M1 \times N1 = 1632 \times 1224$; according to (3), $P_{LF}\_1$ can be calculated, as $P_{LF}\_1 = 50.19\%$; therefore, the adaptive initial size of the superpixels is calculated using (4), which yields $S\_1 = 199$. Similarly, for the host image I2 in Fig. 4-(B1), with the size $M2 \times N2 = 1306 \times 1950$, $P_{LF}\_2 = 39.89\%$, and $S\_2 = 159$; for the host image I3 in Fig. 4-(C1), with the size $M3 \times N3 = 1936 \times 1296$, $P_{LF}\_2 = 59.92\%$, and $S\_3 = 224$. Fig. 4-(A4), (B4), and (C4) show the host image segmentations with the proposed Adaptive Over-Segmentation method, and (a4), (b4), and (c4) show the corresponding detected forgery regions with the proposed Adaptive Over-Segmentation method. We can see that in Fig. 4-(A), with the calculated adaptive size, $S\_1 = 199$, the forgery detection result in Fig. 4-(a4) performs better than the results when the fixed sizes are $S = 150$ and $S = 250$ (which are given in Fig. 4-(a2) and (a3), respectively). In Fig. 4-(B), with the calculated adaptive size $S\_2 = 159$, the forgery detection result in Fig. 4-(b4) is similar to the result in Fig. 4-(b2) when $S = 150$; in addition, it performs better than the results in Fig. 4-(b3) when $S = 250$. In Fig. 4-(C), with the calculated adaptive size, $S\_3 = 224$, the forgery detection result in Fig. 4-(c4) becomes close to the result in Fig. 4-(b3) when $S = 250$, and it performs better than the results in Fig. 4-(b2) when $S = 150$.

As discussed above, the proposed Adaptive Over-Segmentation method can divide the host image into blocks with adaptive initial sizes according to the given host images, with which each image can be determined to be an appropriate block initial size to enhance the forgery detection results. The proposed Adaptive Over-Segmentation method can lead to better forgery detection results compared with the forgery detection methods, which segment the host images into fixed-size blocks and, at the same time, reduce the computational expenses compared with most of the existing forgery detection methods, which segment the host images into overlapping blocks.

### *B. Block Feature Extraction Algorithm*

In this section, we extract block features from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features; however, those features mainly reflect the content of the image blocks, leaving out the location information. In addition, the features are not resistant to various image transformations. Therefore, in this paper, we extract feature points from each image block as block features, and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression.

In recent years, the feature points extraction methods SIFT [20] and SURF [21] have been widely used in the field of computer vision. The feature points extracted by SIFT and SURF were proven to be robust against common image processing operations such as rotation, scale, blurring, and compression; consequently, SIFT and SURF were often used as feature point extraction methods in the existing keypoint-based copy-move forgery detection methods. Christlein et al. [22] showed that the SIFT possessed more constant and better performance compared with the other 13 image feature extraction methods in comparative experiments. As a result, in our proposed algorithm, we chose SIFT as the feature point extraction method to extract the feature points from each image

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



block, and each block is characterized by the SIFT feature points that were extracted in the corresponding block. Therefore, each block feature contains irregular block region information and the extracted SIFT feature points.

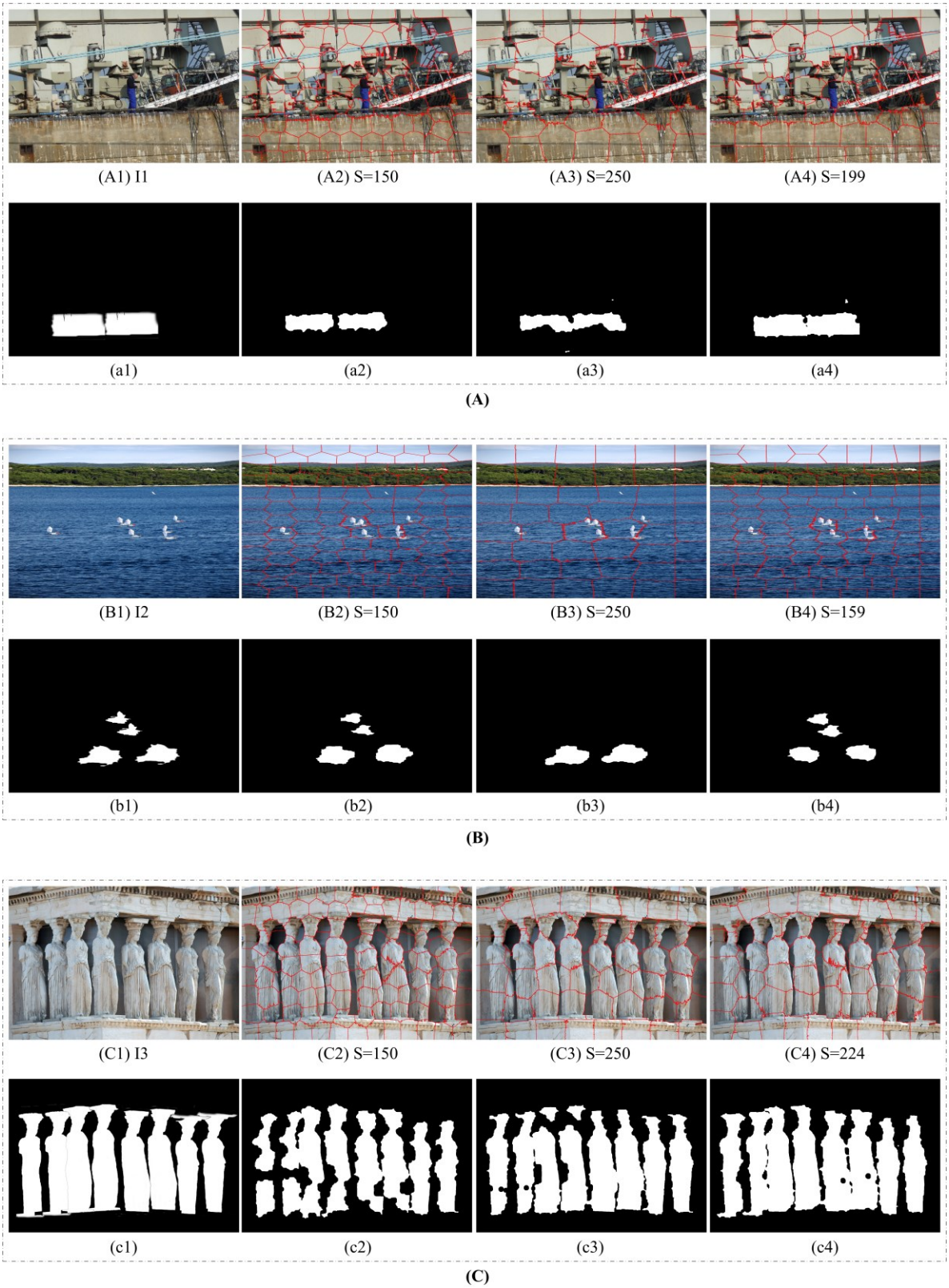


Fig. 4 Superpixels of different initial sizes and the corresponding forgery detection results (A1), (B1), and (C1). The copy-move host images, I1, I2 and I3; (a1), (b1), (c1) The corresponding forgery regions of I1, I2 and I3, respectively. (A2), (B2), (C2) The host images are blocked into superpixels with initial size $S=150$ ; (a2), (b2), (c2) The corresponding detected forgery regions when $S=150$ . (A3), (B3), (C3) The host images are blocked into superpixels with initial size $S=250$ ; (a3), (b3), (c3) The corresponding detected forgery regions when $S=250$ . (A4), (B4), (C4) The host images are blocked into superpixels with the proposed Adaptive

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



Over-segmentation method, by which the initial superpixel sizes are calculated as $S=199$, $S=159$, and $S=224$, respectively; (a4), (b4), (c4) The corresponding detected forgery regions with the proposed Adaptive Over-segmentation method.

### C. Block Feature Matching Algorithm

After we have obtained the block features (BF), we must locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. In our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks. Fig. 5 shows the flowchart of the Block Feature Matching algorithm. First, the number of matched feature points is calculated, and the correlation coefficient map is generated; then, the corresponding block matching threshold is calculated adaptively; with the result, the matched block pairs are located; and finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region. The detailed steps are explained as follows.

**Algorithm: Block Feature Matching algorithm**
**Input:** Block Features (BF);
**Output:** Labeled Feature Points (LFP).
**STEP-1:** Load the Block Features $BF=\{BF_1, BF_2, \ldots$ , where $N$ means the number of image blocks; and calculate the correlation coefficients $CC$ of the image blocks.
**STEP-2:** Calculate the block matching threshold $TR_B$ according to the distribution of correlation coefficients.
**STEP-3:** Locate the matched blocks $MB$ according to the block matching threshold $TR_B$.
**STEP-4:** Label the matched feature points in the matched blocks $MB$ to indicate the suspected forgery regions.

In **STEP-1**, the correlation coefficient $CC$ of the image blocks indicates the number of matched feature points between the corresponding two image blocks. Assuming that there are $N$ blocks after the adaptive over-segmentation, we can generate $N(N-1)/2$ correlation coefficients, which form the correlation coefficient map. Among the blocks, the two feature points are matched when their Euclidean distance is greater than the predefined feature points' matching threshold $TR_p$, which means that the feature point $f_a(x_a, y_a)$ is matched to the feature point $f_b(x_b, y_b)$ only if they can meet the condition defined in (5).

$$d(f_a, f_b)\cdot TR_p \le d(f_a, f_i) \tag{5}$$

where $d(f_a, f_b)$ means the Euclidian distance between the feature points $f_a$ and $f_b$, as defined in (6); $d(f_a, f_i)$ means the Euclidian distances between the keypoints $f_a$ and all of the other keypoints in the corresponding block, as defined in (7), $i$ means the $i^{th}$ feature points and $n$ means the number of feature points in the corresponding block; in addition, $TR_p$ indicates

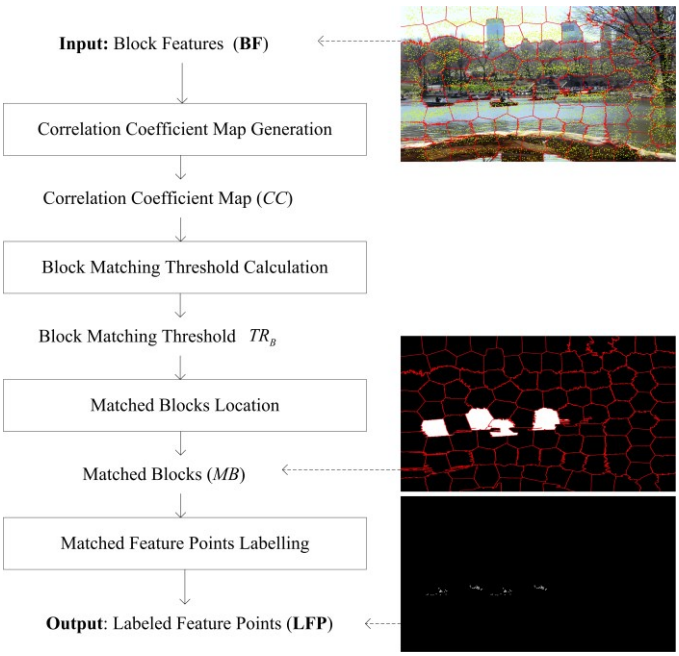


Fig. 5 Flowchart of the Block Feature Matching algorithm

the feature points matching threshold. When $TR_p$ becomes larger, the matching accuracy will be higher, but at the same time, the miss probability will be increased. Therefore, in the experiments, we set $TR_p=2$ to provide a good trade-off between the matching accuracy and miss probability.

$$d(f_a, f_b)=\sqrt{(x_a-x_b)^2+(y_a-y_b)^2} \tag{6}$$

$$d(f_a, f_i)=\sqrt{(x_a-x_i)^2+(y_a-y_i)^2}, i=1,2,...n; i\neq a, i\neq b \tag{7}$$

In **STEP-2**, to calculate the block matching threshold $TR_B$, first the different elements of the correlation coefficients are sorted in ascending order as $CC\_S=\{CC_1, CC_2, CC_3, \cdots\cdots$ , where $t\le N(N-1)/2$. Then, the first derivative and second derivative of $CC\_S$, $\nabla(CC\_S)$ and $\nabla^2(CC\_S)$ as well as the mean value of the first derivative vector $\overline{\nabla(CC\_S)}$ are calculated. Finally, we select the minimum correlation coefficient from among those whose second derivative is larger than the mean value of the corresponding first derivative vector, as defined in (8). The selected correlation coefficient value is defined as the block matching threshold $TR_B$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



$$\nabla^2(CC\_S) > \overline{\nabla(CC\_S)} \tag{8}$$

In **STEP-3**, with the calculated block matching threshold $TR_B$, if the correlation coefficient of the block pair is larger than $TR_B$, the corresponding block pair will be determined to be matched blocks; and in **STEP-4**, the matched feature points in the matched blocks are labeled to indicate the suspected forgery regions.

In the proposed Block Feature Matching algorithm, we have defined two thresholds to match the blocks: the feature points' matching threshold $TR_p$ and the block matching threshold $TR_B$, to avoid possible mismatched features, particularly for those copy-move forgery regions that are similar to the image background. Among the blocks, the two feature points are matched when their Euclidean distance is greater than $TR_p$, which can be adjusted to reduce the falsely matched feature points. Furthermore, the two blocks are only matched when their correlation coefficient is larger than $TR_B$. In summary, in the proposed scheme, with these two thresholds, most of the false matching can be avoided.

### *D. Forgery Region Extraction Algorithm*

Although we have extracted the labeled feature points (LFP), which are only the locations of the forgery regions, we must still locate the forgery regions. Considering that the superpixels can segment the host image very well, we proposed a method by replacing the LFP with small superpixels to obtain the suspected regions (SR), which are combinations of labeled small superpixels. Furthermore, to improve the *precision* and *recall* results, we measure the local color feature of the superpixels that are neighbors to the suspected regions (SR); if their color feature is similar to that of the suspected regions, then we merge the neighbor superpixels into the corresponding suspected regions, which generates the merged regions (MR). Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions. Fig. 6 shows the flow chart of the Forgery Region Extraction algorithm, which is explained in detail as follows.

**Algorithm: Forgery Region Extraction**
**Input:** Labeled Feature Points (LFP)
**Output:** Detected Forgery Regions.
**STEP-1:** Load the Labeled Feature Points (LFP), apply the SLIC algorithm with the initial size *S* to the host image to segment it into small superpixels as feature blocks, and replace each labeled feature point with its corresponding feature block, thus generating the Suspected Regions (SR).
**STEP-2:** Measure the local color feature of the superpixels neighbor to the SR, called neighbor blocks; when their color feature is similar to that of the suspected regions, we merge the neighbor blocks into the corresponding SR, therefore creating the merged regions (MR).
**STEP-3:** Apply the morphological close operation into MR to finally generate the detected forgery regions.

In **STEP-1**, assuming that $LPF = \left\{\left\langle LP_1, \overline{LP_1}\right\rangle, \left\langle LP_2, \overline{LP_2}\right\rangle, \cdots \quad \overline{P_n}\right\rangle\}$, where $\left\langle LP_i, \overline{LP_i}\right\rangle$ represents a matched feature point pair, $i$ means the $i^{th}$ labeled feature point pair, $i = 1, 2, \ldots$, and $n$ is the total number of feature points in LFP; the suspected regions will be $SR = \left\{\left\langle LS_1, \overline{LS_1}\right\rangle, \left\langle LS_2, \overline{LS_2}\right\rangle, \cdots \quad \overline{S_n}\right\rangle\}$. The initial size of the SLIC algorithm *S,* which we used to segment the host image into small superpixels, is related to the size of the host images; in this paper, for high resolution host images, for example, when the size of the host image is approximately $3000 \times 3000$, the initial size is set to $S = 20$ by experiments; while for low-resolution host images, for example, when the size of the host image is approximately $1500 \times 1500$, the initial size is set to $S = 10$ by the experiments.

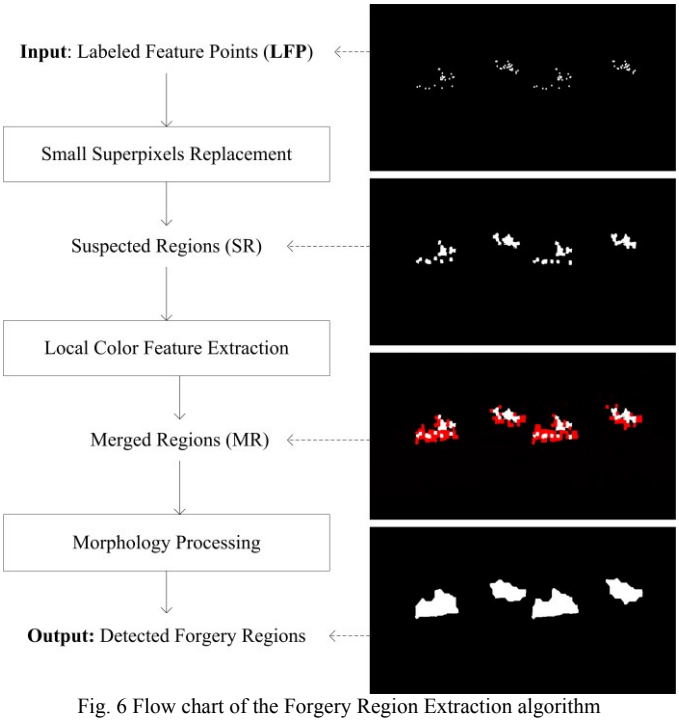


Fig. 6 Flow chart of the Forgery Region Extraction algorithm

In **STEP-2**, for each suspected region $SR_i = \left\langle LS_i, \overline{LS_i}\right\rangle$, the neighboring blocks are defined as $SR_i\_neighbor = \left\langle LS_{i\_\theta}, \overline{LS_{i\_\theta}}\right\rangle$, where $\theta = \{45^\circ, 90^\circ, 135^\circ, 180^\circ, 225^\circ, 270^\circ, 315^\circ, 360^\circ\}$; then, we measure the local color feature of the corresponding suspected region $SR_i$ and its neighboring blocks $SR_i\_neighbor$, using (9) and (10), respectively.

$$\begin{aligned} F_C\_LS_i &= \frac{R(LS_i) + G(LS_i) + B(LS_i)}{3} \\ F_C\_\overline{LS_i} &= \frac{R(\overline{LS_i}) + G(\overline{LS_i}) + B(\overline{LS_i})}{3} \end{aligned} \tag{9}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



$$F_C\_LS_{i\_\theta} = \frac{R(LS_{i\_\theta}) + G(LS_{i\_\theta}) + B(LS_{i\_\theta})}{3}$$
$$F_C\_\overline{LS_{i\_\theta}} = \frac{R(\overline{LS_{i\_\theta}}) + G(\overline{LS_{i\_\theta}}) + B(\overline{LS_{i\_\theta}})}{3} \quad (10)$$

where $R()$ , $G()$ and $B()$ mean calculating the RGB components of the corresponding block, respectively. When the local color feature of the neighboring blocks is similar to that of the corresponding suspected regions, which means that the local feature can meet the condition defined in (11), the neighboring block will be merged into the corresponding suspected region.

$$\left|F_C\_LS_i - F_C\_LS_{i\_\theta}\right| \le TR_{sim}$$
$$\left|F_C\_\overline{LS_i} - F_C\_\overline{LS_{i\_\theta}}\right| \le TR_{sim} \quad (11)$$

where $F_C\_LS_i$ and $F_C\_\overline{LS_i}$ are the local color features of the corresponding suspected region $SR_i$ , $SR_i = \left\langle LS_i, \overline{LS_i} \right\rangle$ ; $F_C\_LS_{i\_\theta}$ and $F_C\_\overline{LS_{i\_\theta}}$ are the local color features of its neighboring blocks $SR_i\_neighbor$ , $SR_i\_neighbor = \left\langle LS_{i\_\theta}, \overline{LS_{i\_\theta}} \right\rangle$ . $TR_{sim}$ is the threshold to measure the similarity between the local color features; in this paper, we set $TR_{sim} = 15$ in the experiments.

Finally, in **STEP-3**, the structural element that we use in the close operation is defined as a circle whose radius is related to the size of the host image. The close operation can fill the gaps in the merged regions and, at the same time, keep the shape of the region unchanged.

## III. Experiments and Discussion

In this section, a series of experiments are conducted to evaluate the effectiveness and robustness of the proposed image forgery detection scheme using adaptive over-segmentation and feature point matching. In the following experiments, the image dataset in [22] is used to test the proposed method. This dataset is formed based on 48 high-resolution uncompressed PNG true color images, and the average size of the images is $1500 \times 1500$. In the dataset, the copied regions are from the categories of living, nature, man-made and mixed, and they range from overly smooth to highly textured; the copy-move forgeries are created by copying, scaling and rotating semantically meaningful image regions. In summary, the dataset has 1826 images in total, which are realistic copy-move forgeries. Therefore, we chose this dataset to objectively evaluate our method. Fig. 7 shows the copy-move forgery detection results of the proposed scheme. In Fig. 7, (a1), (b1), (c1), (d1) and (e1) display the host images, which are forged images that are selected from the dataset; (a2), (b2), (c2), (d2) and (e2) show the corresponding forgery regions; and (a3), (b3), (c3), (d3) and (e3) show the forgery regions that were detected with the proposed scheme.

In the following experiments, the two characteristics *precision* and *recall* [16, 22] are used to evaluate the performance of the proposed forgery detection scheme. *Precision* is the probability that the detected regions are relevant, and it is defined as the ratio of the number of correctly detected forged pixels to the number of totally detected forged pixels, as stated in (12). *Recall* is the probability that the relevant regions are detected, and it is defined as the ratio of the number of correctly detected forged pixels to the number of forged pixels in the ground-truth forged image, as stated in (13).

$$precision = \frac{\left|\Omega \cap \right.}{\left|\Omega\right|} \quad (12)$$

$$recall = \frac{\left|\Omega \cap \right.}{\left|\Omega^{'}\right|} \quad (13)$$

where $\Omega$ means the detected forgery regions with the proposed scheme from the dataset, for example, (a3) ~ (e3) in Fig. 7; and $\Omega^{'}$ means the ground-truth forgery regions of the dataset, for example, (a2) ~ (e2) in Fig. 7.

In addition to the *precision* and *recall*, we give the $F_1$ score as a reference parameter to measure the forgery detection result; the $F_1$ score combines both the *precision* and *recall* into a single value, and it can be calculated using (14).

$$F_1 = 2 \cdot \frac{precison \cdot recall}{precision + recall} \quad (14)$$

To reduce the effect of the randomness of the samples, the average *precision* and *recall* are computed over all of the images in the dataset. We evaluate the method at the pixel level and image level. Though the pixel-level metrics are useful for assessing the general localization performance of the algorithm when the ground-truth data are available, the image-level decisions are especially interesting with respect to the automated detection of manipulated images. At the pixel level, the *precision* and *recall* are calculated by counting the number of pixels in the corresponding region. At the image level, the *precision* is the probability that a detected forgery is truly a forgery, and the *recall* is the probability that a forgery image is detected. In general, a higher *precision* and a higher *recall* indicate superior performance.

Because Christlein et al. [22] have specifically recommended all of the benchmark methods and because we used the same dataset that they provided, we can compare our experimental results with the copy-move detection evaluation results in their paper. We chose several state-of-the-art existing schemes of the block-based forgery detection method and the keypoint-based forgery detection method to compare with our proposed scheme. For example, Bravo [13] and Wang [8, 9] used the block-based forgery detection method; and the SIFT and SURF feature detection-based forgery detection schemes, which are both discussed in [22], are of the keypoint-based forgery detection method. Furthermore, to measure the advantage of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



the proposed Adaptive Over-Segmentation algorithm, we also block the host images with a fixed initial size, which we set to $S = 240$ instead of blocking the host images adaptively; in this situation, the detection results are also calculated.

In the following sections, first the proposed Adaptive Over-Segmentation algorithm is evaluated in Section III-A, and then, the proposed copy-move forgery scheme is evaluated under different types of tests: the baseline test, for example, and the plain copy-move; the geometric transforms, such as scaling and rotation; common signal processing, such as JPEG compression; and the down-sampling forgeries. Section III-B and III-C demonstrate the test results.

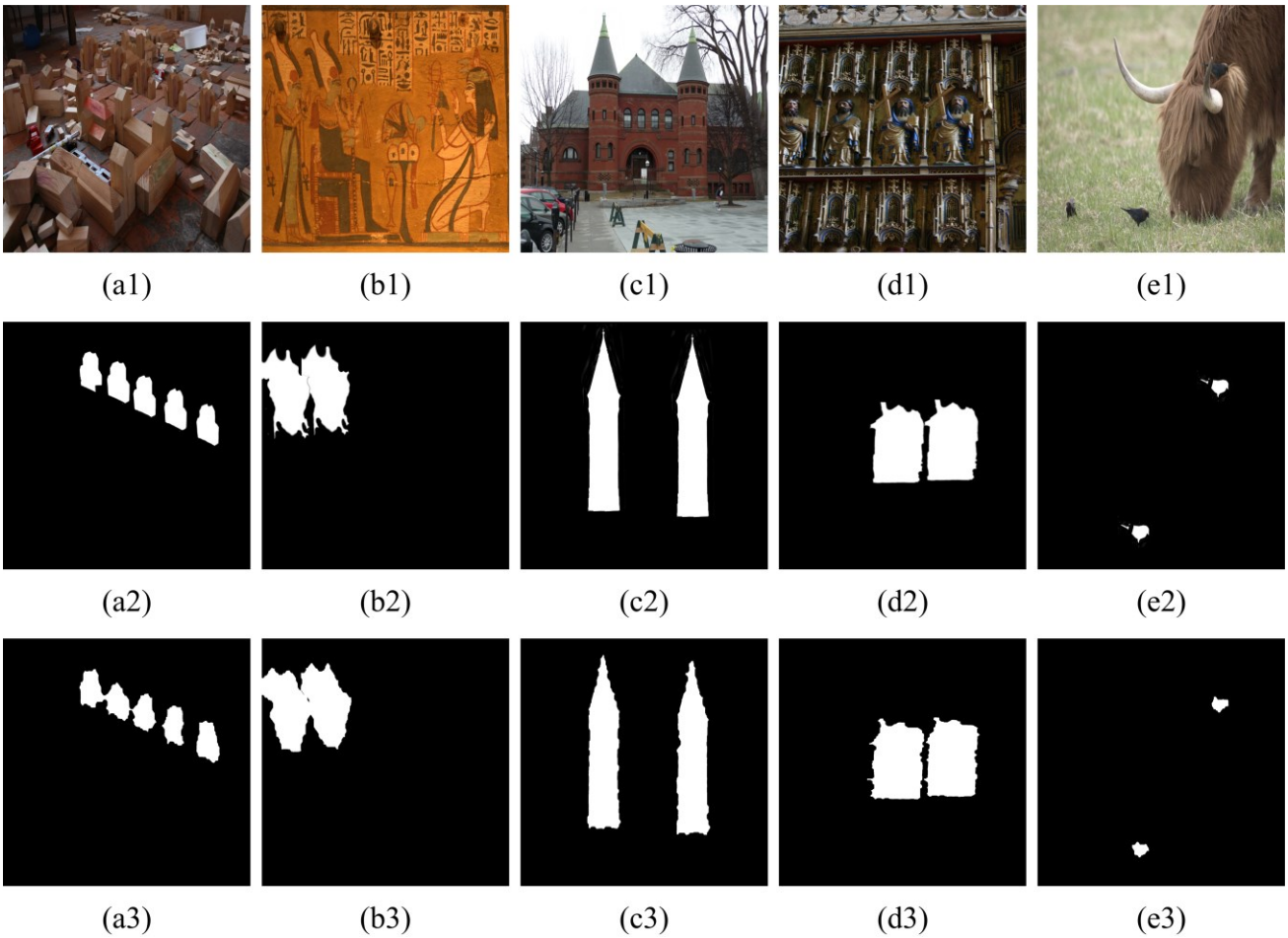


Fig. 7 The copy-move forgery detection results of the proposed scheme (a1) ~ (e1) The five host images from the dataset; (a2) ~ (e2) The ground-truth forgery regions of the corresponding host images; (a3) ~ (e3) The detected forgery regions of the corresponding images, using the proposed forgery detection scheme.

### *A. Evaluation of the Proposed Adaptive Over-Segmentation Algorithm*

As described in Section II-A, the proposed Adaptive Over-Segmentation algorithm can divide the host image into blocks with an adaptive initial size according to the given host images. Compared with other forgery detection methods that segment the host images into fixed-size blocks, the forgery detection results can be improved with the proposed Adaptive Over-Segmentation algorithm. In Fig. 4, three different host images are selected to show the forgery detection results when the host images are blocked into superpixels of different initial sizes. (A1), (B1) and (C1) show the host images I1, I2 and I3, respectively; and (a1), (b1) and (c1) show the corresponding forgery regions (ground-truth). (A2), (B2) and (C2) show the host images being blocked into superpixels with the fixed initial size $S = 150$; and (a2), (b2) and (c2) show the corresponding detected forgery regions. (A3), (B3) and (C3) show the host images being blocked into superpixels with the fixed initial size $S = 250$; and (a3), (b3) and (c3) show the corresponding detected forgery regions. (A4), (B4) and (C4) show the host images being blocked into superpixels with the proposed Adaptive Over-segmentation method, and the initial superpixel sizes are calculated as $S = 199$, $S = 159$ and $S = 224$, respectively; and (a4), (b4) and (c4) show the corresponding detected forgery regions.

Table 1 shows the comparison results for the forgery detection with and without the proposed Adaptive Over-Segmentation algorithm. It can be easily observed that for host image I1, the proposed Adaptive Over-segmentation method can produce more accurate forgery detection results with a higher *Precision=93.85%* and, at the same time, gain a much better *Recall=99.12%*; for host image I2, the proposed Adaptive Over-segmentation method can produce more accurate forgery detection results with higher *Precision=96.60%*; and for host image I3, the proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



Adaptive Over-segmentation method can produce more accurate forgery detection results with higher *Recall=95.19%* and, at the same time, maintain good *Precision=95.28%*. The comparison results indicate that the proposed Adaptive Over-Segmentation algorithm can achieve much better forgery detection results than the other forgery detection methods with fixed-size blocks.

TABLE 1 FORGERY DETECTION RESULTS WITH / WITHOUT THE PROPOSED ADAPTIVE OVER-SEGMENTATION ALGORITHM

| Host Images | | **Fixed-size** ***S = 150*** | **Fixed-size** ***S = 250*** | **Adaptive-size** ***S (I1) = 199*** ***S (I2) = 159*** ***S (I3) = 224*** |
|---|---|---|---|---|
| I1 | *Precision (%)* | 91.44 | 91.91 | **93.85** |
| | *Recall (%)* | 69.99 | 69.74 | **99.12** |
| I2 | *Precision (%)* | 93.07 | 93.26 | **96.60** |
| | *Recall (%)* | **90.75** | 77.43 | 78.90 |
| I3 | *Precision (%)* | **96.90** | 95.59 | 95.28 |
| | *Recall (%)* | 81.49 | 89.46 | **95.19** |

### B. Detection Results under Plain Copy-Move

Basically, we first evaluate the proposed scheme under ideal conditions; in other words, we have 48 original images and 48 forgery images, in which a one-to-one copy-move is implemented. We must distinguish the original and forgery images in this case. Tables 2 and 3 show the detection results for the 96 images when under plain copy-move, at the image and pixel levels, respectively. From Table 2, it can be easily observed that our scheme can achieve *precision=96%* and *recall=100%;* thus $F_1 = 97.96\%$ at the image level, which is much better than the existing state-of-the-art schemes. In Table 3, at the pixel level, our scheme can achieve *precision=97.22%* and *recall=83.73%;* thus $F_1 = 89.97\%$, and it can be easily observed that our proposed scheme performs much better than the keypoint-based forgery detection methods, SIFT [15, 16] and SURF [17, 19]. At the same time, it performs similarly to the block-based forgery detection methods, i.e., those of Bravo [13] and Wang [8, 9]. In addition, we can see that the proposed scheme with the adaptive over-segmentation method performs better than with fixed-size blocking, at both the image and pixel levels.

In some special cases, it is possible that two copy-move regions could be assigned into one single irregular region. and hence, it would be impossible to be detected for the two subsequent situations that occur together: 1. the two duplicated regions are very close to one another or connected; and 2. the size of the connected regions is smaller than the Initial Block Size S (which is defined in Eq. (4) in the proposed Adaptive Over-Segmentation Algorithm). However, the possibility of both situations occurring together is quite low and can be ignored because this circumstance means that the two copy-move forgery regions are extremely small and close. According to our experimental results, we have tested a total of 1824 images in various situations, which are from the Image Manipulation Dataset [22], and there are no two regions that are assigned into one single region.

TABLE 2 DETECTION RESULTS UNDER PLAIN COPY-MOVE AT IMAGE LEVEL

| **Methods** | ***Precision*** **(%)** | ***Recall*** **(%)** | $F_1$ **(%)** |
|---|---|---|---|
| Bravo [13] | 87.27 | 100 | 93.20 |
| Wang [8, 9] | 92.31 | 100 | 96.00 |
| SIFT [15, 16] | 88.37 | 79.17 | 83.52 |
| SURF [17, 19] | 91.49 | 89.58 | 90.53 |
| *Proposed Scheme – Fixed Size Blocking* | 95.92 | 97.92 | 96.91 |
| *Proposed Scheme – Adaptively Blocking* | **96** | **100** | **97.96** |

TABLE 3 DETECTION RESULTS UNDER PLAIN COPY-MOVE AT THE PIXEL LEVEL

| **Methods** | ***Precision*** **(%)** | ***Recall*** **(%)** | $F_1$ **(%)** |
|---|---|---|---|
| Bravo [13] | 98.81 | 82.98 | 89.34 |
| Wang [8, 9] | 98.69 | 85.44 | 90.92 |
| SIFT [15, 16] | 60.80 | 71.48 | 63.10 |
| SURF [17, 19] | 68.13 | 76.43 | 69.54 |
| *Proposed Scheme – Fixed Size Blocking* | 89.87 | 75.6 | 82.12 |
| *Proposed Scheme – Adaptively Blocking* | **97.22** | **83.73** | **89.97** |

### C. Detection Results under Different Transforms

In addition to the plain copy-move forgery, we have tested our proposed scheme when the copied regions are distorted by various attacks. In this case, the forged images are generated by using each of the 48 images in the dataset, and the copied regions are attacked by geometric distortions that include scaling and rotation and common signal processing such as JPEG compression.

1) **Down-Sampling:** All 48 of the forged host images in the dataset are scaled down from 90% to 10% in steps of 20%. In this case, we must test a total of $48 \times 5 = 240$ images.
2) **Scaling:** The copied regions are scaled with the scale factor varying from 91% to 109%, in steps of 2%, and with the scale factor of 50%, 80%, 120% and 200% as well. In this case, we must test a total of $48 \times 14 = 672$ images.
3) **Rotation:** The copied regions are rotated with the rotation angle varying from 2º to 10º, in steps of 2º, and with the rotation angles of 20º, 60º and 180º as well. In this case, we must test a total of $48 \times 8 = 384$ images.
4) **JPEG compression:** The forgery images are JPEG compressed with the quality factor varying from 100 to 20, in steps of -10. In this case, we must test a total of $48 \times 9 = 432$ images.

Figs. 8, 9, and 10 show the detection results at the pixel level when under different attacks: (a) Down-sampling, (b) Scaling, (c) Rotation, and (d) JPEG Compression. Here, the results that are represented in blue and marked 'Proposed' indicate the results of the *Proposed Scheme With Adaptive Blocking*. The results that are represented in yellow and marked 'RSIFT'

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



indicate the results of the *Proposed Scheme with Fixed Size Blocking*. The results that are represented in green and red and marked as 'SIFT' and 'SURF' indicate the results of the keypoint-based forgery detection methods based on SIFT [15, 16] and SURF [17, 19], respectively; and the results that are represented in pink and sky-blue and marked as 'Bravo' and 'Circle' indicate the results of the block-based forgery detection methods proposed by Bravo and Nandi [13] and by Wang et al. [8, 9], respectively.

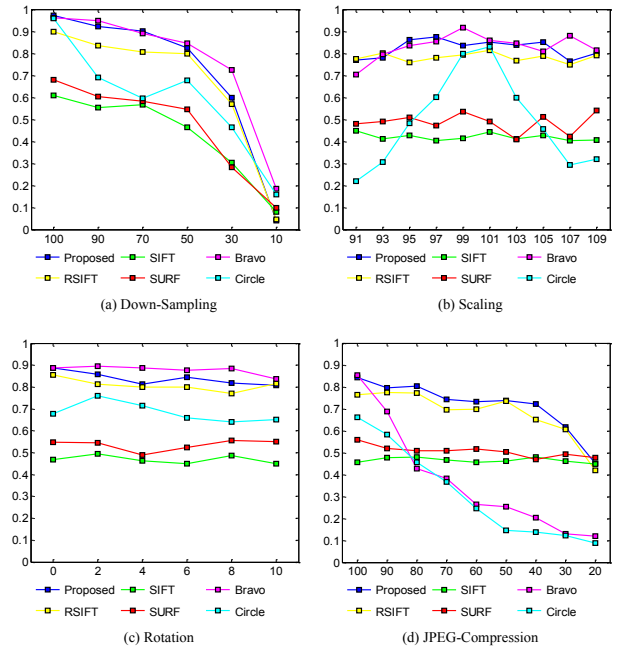


Fig. 8 *Precision* results at the pixel level (a) Down-sampling; (b) Scaling; (c) Rotation; and (d) JPEG Compression.

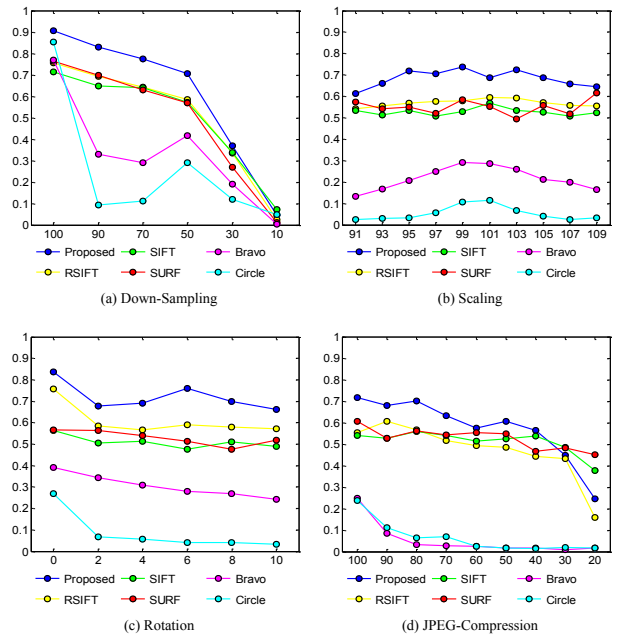


Fig. 9 *Recall* results at the pixel level (a) Down-sampling; (b) Scale; (c) Rotation; and (d) JPEG Compression.

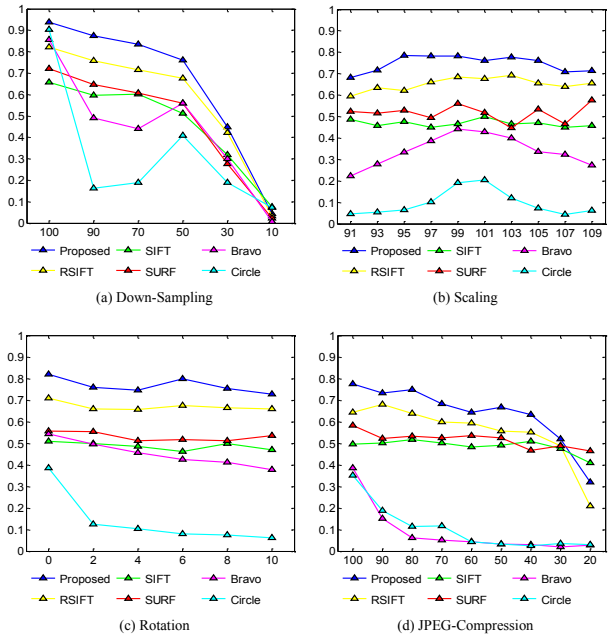


Fig. 10 $F_1$ scores at the pixel level (a) Down-sampling; (b) Scale; (c) Rotation; and (d) JPEG Compression.

In Fig. 8 ~ 10, the x-axis in (a) represents the factor of down-sampling, (b) represents the scale factor, (c) represents the rotation angle, and (d) represents the quality factor. Fig. 8 shows the *precision* results of the proposed scheme compared with the existing methods; it can be easily observed that the *precision* of the proposed scheme exceeds that of the existing keypoint-based methods, SIFT [15, 16] and SURF [17, 19], by a large amount and is as good as that of the existing block-based methods (the schemes proposed by Bravo and Nandi [13] and by Wang et al. [8, 9]) under various attacks, including geometric distortions and common signal processing. Moreover, according to the precision results, the proposed scheme with the adaptive over-segmentation method performs better than that with the fixed-size blocking.

At the same time, Fig. 9 shows the *recall* results of the proposed scheme compared with the existing methods. It can be easily observed that the *recall* of the proposed scheme is much better than that of the existing methods when under various attacks; this finding is expected because in our scheme, we proposed the Forgery Region Extraction algorithm to locate the forgery regions, which replace the feature points with small superpixels as feature blocks and then merge the neighboring blocks with similar local color features into the feature blocks. The Forgery Region Extraction algorithm can help greatly reduce the possibility of the forgery being undetected and can thus improve the *recall* by a large amount.

Fig. 10 shows the $F_1$ scores, which combine both the *precision* and *recall* into a single value, for the proposed scheme compared with the existing methods. This figure indicates that the forgery detection result of the proposed scheme is better than that of the existing state-of-the-art methods when under the various attacks.

Although our rotation experiments only involve rotation with very small angles, our proposed method can work well against

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2015.2423261, IEEE Transactions on Information Forensics and Security



any rotation angle because our block features are extracted by the SIFT algorithm, which is well known for its robustness to scale and rotation invariance. We have also conducted the experiments for copy-move forgery regions with large rotation angles: the results turn out to be similar and are very good.

## IV. Conclusions

Digital forgery images created with copy-move operations are challenging to detect. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over-Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labeled feature points are replaced with small superpixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions.

We demonstrate the effectiveness of the proposed scheme with a large number of experiments. Experimental results show that the proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling, compared with the existing state-of-the-art copy-move forgery detection schemes. Future work could focus on applying the proposed forgery detection scheme based on adaptive over-segmentation and feature-point matching on other types of forgery, such as splicing or other types of media, for example, video and audio.

## Acknowledgment

The authors would like to thank the reviewers for their valuable comments.

## References

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *in Proceedings of Digital Forensic Research Workshop*, 2003.

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

[3] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, 2006, pp. 746-749.

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *Multimedia and Expo, 2007 IEEE International Conference on*, 2007, pp. 1750-1753.

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

[6] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Computer Science and Software Engineering, 2008 International Conference on*, 2008, pp. 926-930.

[7] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, 2009, pp. 1053-1056.

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in *Multimedia Information Networking and Security, 2009. MINES'09. International Conference on*, 2009, pp. 25-29.

[9] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," *Acta Automatica Sinica,* vol. 35, pp. 1488-1495, 2009.

[10] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," *WSEAS Transactions on Signal Processing,* vol. 5, pp. 188-197, 2009.

[11] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding*, 2010, pp. 51-65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," *Ieee Transactions on Information Forensics and Security,* vol. 8, pp. 1355-1370, Aug 2013.

[13] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, 2011, pp. 1880-1883.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*, 2008, pp. 272-276.

[15] X. Y. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," *Ieee Transactions on Information Forensics and Security,* vol. 5, pp. 857-867, Dec 2010.

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

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

[18] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," *Information Forensics and Security, IEEE Transactions on,* vol. 7, pp. 1018-1028, 2012.

[19] B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," *IJCSI International Journal of Computer Science Issues,* vol. 8, 2011.

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

[21] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Computer Vision–ECCV 2006*, ed: Springer, 2006, pp. 404-417.

[22] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *Ieee Transactions on Information Forensics and Security,* vol. 7, pp. 1841-1854, Dec 2012

[23] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," *IEEE Trans Pattern Anal Mach Intell,* vol. 34, pp. 2274-82, Nov 2012.