Digital Signal Processing 39 (2015) 50–62

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

# Effective composite image detection method based on feature inconsistency of image components

Wu-Chih Hu *, Jing-Siou Dai, Jhih-Syuan Jian

*Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Taiwan*

ARTICLE INFO

*Article history:*
Available online 29 January 2015

*Keywords:*
Composite image
Tampering detection
Image component
Feature inconsistency
Sensor pattern noise

ABSTRACT

This paper proposes an effective composite image detection method that uses the feature inconsistency of image components of the composite image to detect tampered regions. The composite image is first divided into image components. Next, the variance of the noise remaining after de-noising in each image component is calculated and used as a feature. Finally, tampered regions are detected using this feature based on a tampering detection rule. Experimental results show that the proposed method has good composite image detection performance.



## 1. Introduction

Digital images have become ubiquitous. With the availability of powerful image processing technology and digital image editing tools, digital images have become easier to duplicate and manipulate without degrading quality or leaving obvious visual clues. Image forgery has become a serious problem, and thus the authentication of images has become increasingly important. Therefore, accurate and robust detection of image forgery is desirable.

Image forensic methods can be roughly divided into those based on active and passive technologies [1–3]. The active forensic approach is a non-blind approach that extracts prior inserted information from a digital image (e.g., digital watermarks or signatures) to determine authenticity. The image is recognized as having been tampered when the embedded information has changed. Image watermarking [4–6] is a popular active technique among non-blind approaches. Image watermarking embeds a hidden watermark at recording time that is extracted later to verify image authenticity. Hu et al. [7] proposed a novel image forgery detection method that uses the difference of singular values based on discrete wavelet transform (DWT)-discrete cosine transform (DCT)-singular value decomposition (SVD)-based image watermarking [8] and alpha mattes [9,10] to determine the tampered foreground or background image. This method works well for images manipulated using image matting.

The passive forensic approach is a blind approach with no supplementary information used. That is, blind approaches determine the feature consistency of an image without the use of embedded information. Region duplication detection, a common type of image forgery detection, includes copy–move forgery detection [11–14] and composite image detection [15–21]. Compared to active forensic approaches, passive ones can authenticate an image without a priori knowledge. Therefore, passive forensic approaches are more practical.

In passive forensic approaches, copy–move forgery detection and composite image detection are commonly considered. Copy–move forgery detection usually uses a block-based scheme to detect image forgery. An image is first divided into fixed-size overlapping blocks and then features of the blocks are extracted and represented as feature vectors. Next, the feature vectors are sorted in lexicographical order to make similar blocks close to each other. Finally, duplicate blocks are filtered out using a similarity measure. Chang et al. [22] proposed a forgery detection algorithm that uses a multi-region relation for copy–move forgery detection. It works well for images manipulated using image inpainting.

Composite image detection has no reference regions for checking duplicate regions. In general, a composite image is created by taking a region from a source image and pasting it into a target image after performing geometric operations (such as scaling, rotation, and morphing). The composite image contains tampered and untampered regions. Feature inconsistency is used for the tampering detection, such as feature inconsistency based on noise [15,16,29], JPEG compression [17–20], and shadows [21]. Composite image detection is more difficult than copy–move forgery detection.

Mahdian and Saic [15] proposed a composite image detection method based on local noise level inconsistencies. One-level DWT is first applied to the composite image to obtain the *HH* sub-band image. Next, the obtained *HH* sub-band image is divided into fixed-size non-overlapping blocks. The noise standard deviation of each

* Corresponding author.
*E-mail addresses:* wchu@npu.edu.tw, wuchih.hu@gmail.com (W.-C. Hu), amshuo@hotmail.com (J.-S. Dai), diablo791220@gmail.com (J.-S. Jian).

http://dx.doi.org/10.1016/j.dsp.2015.01.006
1051-2004/

block is calculated using the widely used median-based method. The homogeneity condition is used to segment the image into several homogeneous sub-regions based on the obtained noise standard deviation of each block. Finally, the region merging algorithm is applied to neighboring blocks based on block similarity with a given threshold to detect tampered regions. Compared to the method proposed by Popescu [16], the method in [15] uses a more precise estimation of noise level. The main drawback of Popescu's method is that in order to estimate the local noise variance of a single-channel image, the local kurtosis values of the noiseless image need to be known. The estimation of kurtosis introduces numerical errors and decreases performance. However, in the method in [15], additive white Gaussian noise is necessary, and the accuracy of tampering detection is influenced by the given threshold and additive noise level. Furthermore, based on the authors' suggestion [15], this method is useful as a supplement to other forgery detection methods rather than a standalone forgery detector.

Fan et al. [29] proposed a new tool for manipulation detection, which correlates statistical image noise features with selected features from three EXchangeable Image File format (EXIF) header features. Each EXIF feature is formulated as a weighted sum of selected statistical image noise features based on sequential floating forward selection, the weights are then solved as a least squares solution for modeling the correlation between the intact image and the corresponding EXIF header. Image manipulations like brightness and contrast adjustment can affect these noise features and lead to enlarged numerical difference between each actual and its estimated EXIF feature from the noise features. However, EXIF-noise-based tampering detection method is only useful on EXIF images.

Zuo et al. [17] proposed a composite image detection method based on the traces of re-sampling and JPEG compression. An image is first divided into overlapping blocks. Next, a block measure factor is defined and evaluated. The block measure factor contains both the re-sampling characteristics and JPEG compression characteristics of each block. Finally, the block measure factor is applied to detect tampered regions. Unlike other JPEG image forgery detection methods [18–20], when the quality factor of double compression is smaller than the primary quality factor, the method in [17] can still work well. However, based on the authors' suggestion [17], this method becomes ineffective when the composite image is composed of two uncompressed images, and the tampered regions are not subjected to geometric operations.

Liu et al. [21] proposed a composite image detection method based on the photometric consistency of illumination in shadows. The color characteristics of shadows measured in terms of the shadow matte value are first formulated. Next, the shadow boundaries and the penumbra shadow region of the image are extracted. Then, the shadow matte values for each of the sampled shadows in an image are estimated and tested. Finally, the feature consistency is used to detect image tampering. Because this method assumes a single distant light source, its application is limited. Furthermore, this method fails when the composite shadows are consistent with the real target shadows. Moreover, based on authors' suggestion [21], although this method can identify whether an image is tampered, it cannot determine which part of the composite image has been doctored.

Compared to above mentioned methods based on feature inconsistency with noise, JPEG compression, or shadows, sensor pattern noise (SPN) is the result of the imperfection of digital image acquisition equipment and it is relatively stable feature. SPN can be considered as a sort of camera fingerprint and used as such to accomplish forgery detection or image identification tasks. SPN can be estimated using the method developed by Lukáš et al. [23]. SPN is the difference between the original image and its de-noised version. Therefore, SPN-based feature inconsistency is used to obtain tampering detection in this paper.

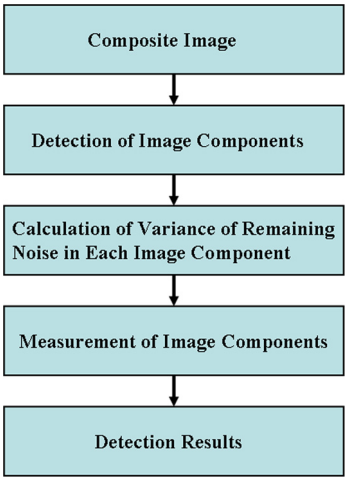


**Fig. 1.** Block diagram of proposed method.

The noise calculation is an important issue in SPN-based tampering detection methods. It is crucial for the detection performance. However, in the presented SPN-based tampering detection methods, the non-overlapping blocks are usually used as image segmentation, but they would obtain tampered regions with jagged shapes. To obtain more accurate tampered regions, a suitable form of image segmentation is necessary to obtain more relational regions for detecting fine contours of tampered regions. Image component is a kind of image segmentation. Therefore, image-component-based tampering detection method is proposed in this paper to obtain fine contours of tampered regions. It is worth mentioning that image-component-based composite image detection is first proposed.

The present study proposes an effective composite image detection method based on the feature inconsistency of image components. In the proposed method, an image is first divided into image components using the adaptive component detection method [10]. Next, the variance of the noise remaining after de-noising in each image component is evaluated. The variance of the remaining noise is a kind of SPN. Finally, tampered regions are detected using the variance of the remaining noise of image components based on a tampering detection rule. The proposed method can obtain fine contours of tampered regions, unlike methods based on non-overlapping blocks, which obtain rough contours. Experimental results show that the proposed method performs well in terms of composite image detection.

The rest of this paper is organized as follows. The proposed image-component-based composite image detection method is described in Section 2. Section 3 presents experimental results and their evaluations. Finally, conclusions are given in Section 4.

## 2. Image-component-based composite image detection

Because composite image detection has no reference regions for checking duplicate regions, feature inconsistency is usually used to detect tampered regions. Sensor pattern noise (SPN) is the result of the imperfection of digital image acquisition equipment and is relatively stable. Therefore, the variance of the remaining noise is used as the feature to obtain the tampering detection, where the variance of the remaining noise is a kind of SPN. Image-component-based tampering detection is proposed to obtain fine contours of tampered regions. Fig. 1 shows a block diagram of the proposed composite image detection method.

In the proposed method, the image components are obtained using the adaptive component detection method [10]. The mean

(a) (b)

**Fig. 2.** Detection of image components. (a) Composite image and (b) obtained image components.

shift algorithm [24] and spectral segmentation with the $k$-means algorithm based on the eigenvectors of the matting Laplacian matrix [25] are used for adaptive component detection.

The mean shift algorithm is briefly described below. A special class of radially symmetric kernels satisfying $K(x) = c_{k,d}k(\|x\|^2)$ is used, where $c_{k,d} > 0$ is chosen such that:

$$\int_0^\infty K(x)dx = \int_0^\infty c_{k,d}k\big(\|x\|^2\big)dx = 1 \tag{1}$$

$k(x)$, the profile of the kernel, is a monotonically decreasing function defined only for $x \geq 0$. Given the function $g(x) = -k'(x)$ for a profile, the kernel $G(x)$ is defined as $G(x) = c_{k,d}g(\|x\|^2)$.

For $n$ data points $x_i$, $i = 1, \ldots, n$, in the $d$-dimensional space $R^d$, the mean shift is defined as in (2), where $x$ is the center of the kernel (window) and $h$ is a bandwidth parameter.

$$m_{h,G(x)} = \left(\sum_{i=1}^{n} x_i g\left(\left\|\frac{x - x_i}{h}\right\|^2\right)\right) \Big/ \left(\sum_{i=1}^{n} g\left(\left\|\frac{x - x_i}{h}\right\|^2\right)\right) - x \tag{2}$$

The mean shift method is guaranteed to converge to a nearby point where the estimate has the zero gradient. The center position of kernel $G$ can be updated iteratively using (3), where $y_1$ is the center of the initial position of the kernel.

$$y_{j+1} = \sum_{i=1}^{n} x_i g\left(\left\|\frac{y_j - x_i}{h}\right\|^2\right) \Big/ \sum_{i=1}^{n} g\left(\left\|\frac{y_j - x_i}{h}\right\|^2\right), \quad j = 1, 2, \ldots \tag{3}$$

The number of clusters in the image is used to obtain the image components by using spectral segmentation with the $k$-means algorithm based on the eigenvectors of the matting Laplacian matrix. The matting Laplacian matrix is defined as a sum of matrices $L = \sum_q A_q$, each of which contains the affinities among pixels inside a local window $w_q$, where $\delta_{ij}$ is the Kronecker delta; $\mu_q$ is a $3 \times 1$ mean color vector in the window $w_q$ around pixel $q$; $\sum_q$ is a $3 \times 3$ covariance matrix in a given window; $|w_q|$ is the number of pixels in a given window; $I_{3\times3}$ is a $3 \times 3$ identity matrix; $I_i$ and $I_j$ are $3 \times 1$ color vectors in the window $w_q$; and $\varepsilon$ is a small positive constant.

$$A_q(i,j) = \begin{cases} \delta_{ij} - \frac{1}{|w_q|}(1 + (I_i - \mu_q)^T \\ (\sum_q + \frac{\varepsilon}{|w_q|}I_{3\times3})^{-1}(I_j - \mu_q)), & (i,j) \in w_q \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

The adaptive component detection method has an accuracy of about 94% under low-, medium-, and high-complexity image segmentation [10], where accurate component detection is defined as each detected component being only a part of the foreground or background. Fig. 2 shows the image components obtained using adaptive component detection. As can be seen, the eagle was accurately segmented.

The algorithm of the proposed image-component-based composite image detection is given below.

Step 1: Transform image $I$ from the RGB color space into the HSV color space to obtain image.

Step 2: Apply adaptive component detection to image $I_V$ to obtain image components $I_V^k$, $k \in [1, n]$.

Step 3: Apply down-sampling to $I_V^k$ to obtain $I_{V,down}^k$.

Step 4: Apply the one-level DWT to image $I_V$ to obtain sub-band image $I_{V,HH}$.

Step 5: Apply the lower–upper–middle (LUM) filter [26] to image $I_{V,HH}$ to obtain the de-noised image $(I_{V,HH})_{denoise}$.

Step 6: Calculate the remaining noise using (5).

$$(I_{V,HH})_R = I_{V,HH} - (I_{V,HH})_{denoise} \tag{5}$$

Step 7: Calculate the variance of the remaining noise in each image component $Var_{re\_noise}^k$ based on $I_{V,down}^k$ and $(I_{V,HH})_R$.

Step 8: Calculate the measure quality ($MQ$) using (6), where $\max(Var_{re\_noise}^k)$ is the maximum one within all $Var_{re\_noise}^k$. If $MQ \geq Th_Q$, then the tested image is a tampered image and go to Step 9; otherwise it is not a tampered image and go to Step 13.

$$MQ = \max\big(Var_{re\_noise}^k\big) \Big/ \frac{1}{n}\sum_{k=1}^{n} Var_{re\_noise}^k \tag{6}$$

Step 9: Apply the normalization to the obtained variances of the remaining noise of image components to obtain $\tilde{V}ar_{re\_noise}^k$, that is, $0 \leq \tilde{V}ar_{re\_noise}^k \leq 1$. Fig. 3 shows the $\tilde{V}ar_{re\_noise}^k$ for Fig. 2(b).

Step 10: Select the image component with maximum $\tilde{V}ar_{re\_noise}^k$ ($\tilde{V}ar_{re\_noise}^k = 1$) as the tampered image component, and select image components with $\tilde{V}ar_{re\_noise}^k \geq Th_C$ as candidate tampered image components.

Step 11: If candidate tampered image components are adjacent to tampered image components, mark them as tampered and removed them from the list of candidate tampered image components.

Step 12: Collect all the tampered components and then apply up-sampling to obtain the tampered regions in image $I$.

Step 13: Show the result of composite image detection.

In the proposed algorithm of image-component-based composite image detection, down-sampling operation in Step 3 is applied to obtain the same size of sub-band image obtained using one-level DWT operation in Step 4. And, up-sampling operation in Step 12 is applied to obtain the original size of tested image $I$. Furthermore, the reason of calculating $Var^k_{re\_noise}$ using $I^k_{V,down}$ and $(I_{V,HH})_R$ is that these two images are with same size (that is, they are both 1/4 tested image $I$) and it can effectively reduce computational cost. Besides, thresholds $Th_Q = 4.0$ and $Th_C = 0.3$ are set from experience, where the value of $Th_C$ is decided the numbers of candidate tampered image components.

Because the image components are obtained using spectral segmentation with the $k$-means algorithm based on the eigenvectors of the matting Laplacian matrix, there will be broken or incomplete tampered regions. Therefore, a refinement scheme is proposed to obtain more complete tampered regions. Object region refinement with a $3 \times 3$ mask is used to scan the results of tampering detection. Each pixel of untampered regions is checked for whole image to obtain $M_1$ image if the up and down pixels of tested pixel are both the pixels of tampered regions, and this pixel is remarked as a pixel of tampered regions. Each pixel of untampered regions is checked for whole image to obtain $M_2$ image if the left and right pixels of tested pixel are both pixels of tampered regions, and this pixel is remarked as a pixel of tampered regions. Next, $M_1$ and $M_2$ are merged using the "OR" operator. Next, a hole-filling scheme is used to fill the holes in tampered regions. The results of this procedure contain only tampered regions and residual small regions. In this paper, the residual small regions are defined as noise regions. The fast 4-connected component labeling method [27] is used to label each isolated region, whose size is calculated. An isolated region is removed if its area is smaller than the given threshold $Th_r$. The residual small regions are thus removed, leaving only tampered regions. Fig. 4 shows the results obtained using the proposed tampering detection method.

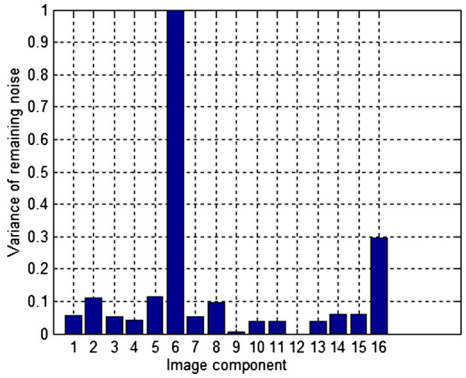


**Fig. 3.** Normalization of variances of the remaining noise of image components for Fig. 2(b).

As shown, the proposed refinement scheme effectively produces more complete tampered regions.

## 3. Experimental results

Performance of the proposed method was evaluated using the own dataset, JPEG compression dataset, and CASIA v1.0 dataset [30]. The algorithm was implemented in Matlab R2011a.

### 3.1. Performance evaluation in own dataset

In the experiments, six composite images were used to evaluate the performance of the proposed tampering detection method. These six composite images look like realistic images, and human inspection may fail.

In order to illustrate the performance of the proposed method, several criteria, namely sensitivity $S_e$, specificity $S_p$, and spatial accuracy $S_a$ [28], were adopted. The sensitivity $S_e$ (true positive rate), specificity $S_p$ (true negative rate) and spatial accuracy $S_a$ are defined in (7)–(9), respectively, where $TP$ is the total number of true positive pixels, $FP$ is the total number of false positive pixels, $TN$ is the total number of true negative pixels, and $FN$ is the total number of false negative pixels. Perfect tampering detection would produce sensitivity, specificity, and spatial accuracy values of 1. The ground truth of the tested composite image was segmented manually.

$$S_e = TP/(TP + FN) \tag{7}$$

$$S_p = TN/(TN + FP) \tag{8}$$

$$S_a = 1 - \big((FP + FN)/(TP + FN)\big) \tag{9}$$

Figs. 5–10 show the tampering detection of various images. Fig. 5 is the tampering detection of image with eagle, where Fig. 5(a) is the target image with JPEG format; Fig. 5(b) is the source image with JPEG format; Fig. 5(c) is the composite image with BMP format; Fig. 5(d) is the image components; Fig. 5(e) is the normalization of variances of remaining noise of image components; and Fig. 5(f) is the obtained result of tampering detection using the proposed method.

Fig. 6 is the tampering detection of image of beach, where Fig. 6(a) is the target image with JPEG format; Fig. 6(b) is the source image with BMP format; Fig. 6(c) is the composite image with BMP format; Fig. 6(d) is the image components; Fig. 6(e) is the normalization of variances of remaining noise of image components; and Fig. 6(f) is the obtained result of tampering detection using the proposed method.

Fig. 7 is the tampering detection of Pyramid image, where Fig. 7(a) is the target image with JPEG format; Fig. 7(b) is the source image with JPEG format; Fig. 7(c) is the composite image with JPEG format; Fig. 7(d) is the image components; Fig. 7(e) is

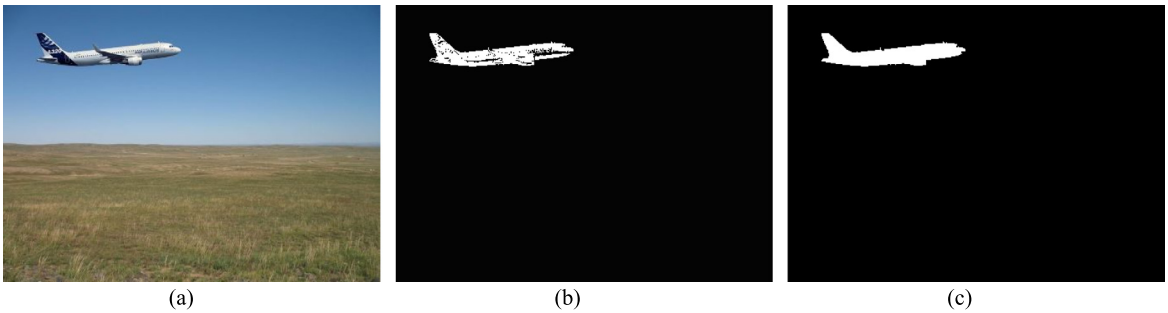


**Fig. 4.** Results obtained using refinement scheme. (a) Tampered image and results obtained using proposed method (b) without and (c) with refinement scheme.

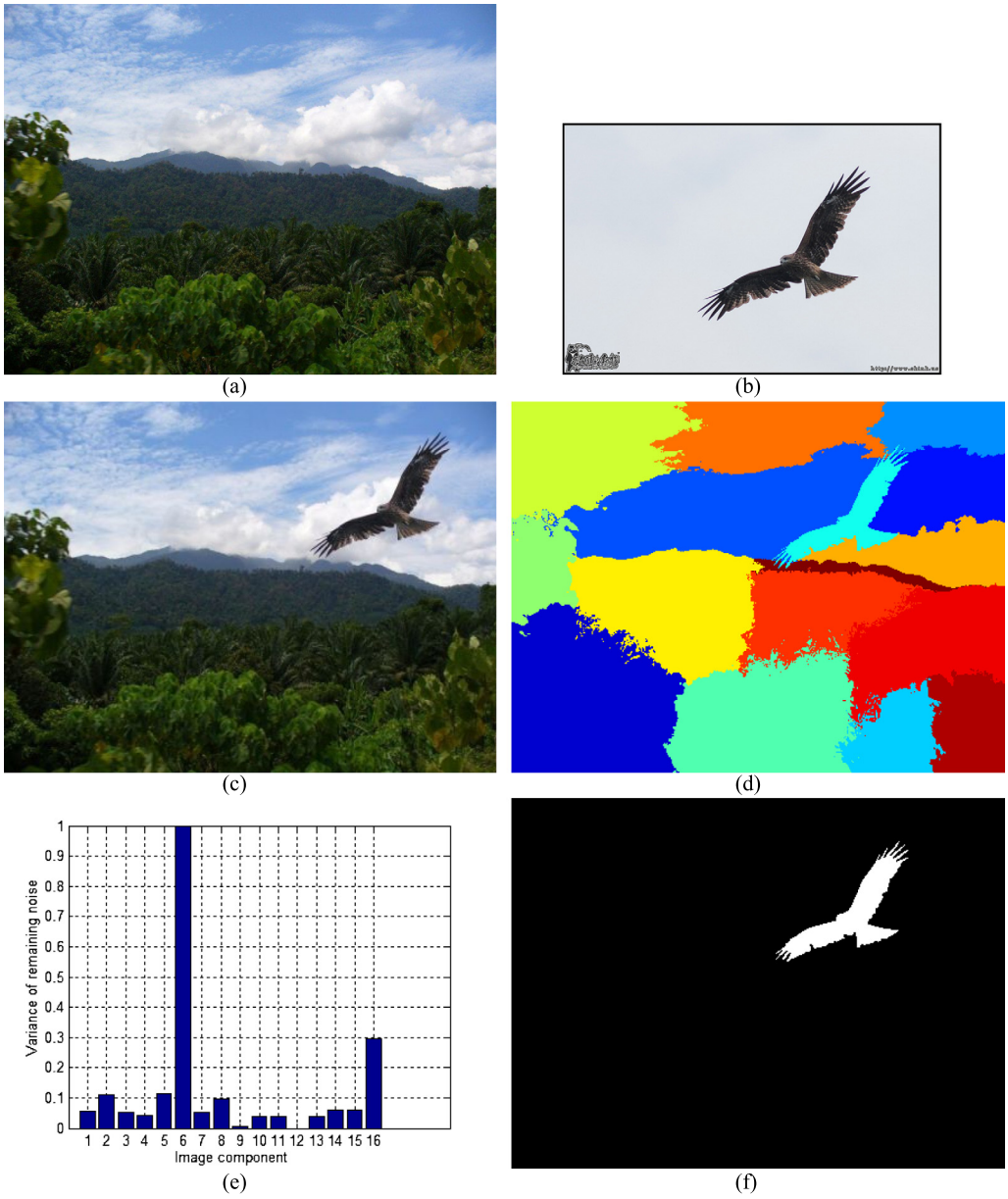


**Fig. 5.** Tampering detection of image with eagle. (a) Target image, (b) source image, (c) composite image, (d) image components, (e) normalization of variances of remaining noise, and (f) detected tampered region.

the normalization of variances of remaining noise of image components; and Fig. 7(f) is the obtained result of tampering detection using the proposed method. Besides, the tampered region is about 50% area of the composite image and the foreground in the target image is entirely covered by tampered region.

Fig. 8 is the tampering detection of image with sky, where Fig. 8(a) is the target image with BMP format; Fig. 8(b) is the source image with BMP format; Fig. 8(c) is the composite image with BMP format; Fig. 8(d) is the image components; Fig. 8(e) is the normalization of variances of remaining noise of image components; and Fig. 8(f) is the obtained result of tampering detection using the proposed method.

Fig. 9 is the tampering detection of image with highway, where Fig. 9(a) is the target image with BMP format; Fig. 9(b) is the source image with JPEG format; Fig. 9(c) is the composite image with JPEG format; Fig. 9(d) is the image components; Fig. 9(e) is the normalization of variances of remaining noise of image components; and Fig. 9(f) is the obtained result of tampering detection using the proposed method. Besides, the source image was deformed and rotated and then copied into the target image to form the composite image.

Fig. 10 is the tampering detection of image with butterfly, where Fig. 10(a) is the target image with BMP format; Fig. 10(b) is the source image with BMP format; Fig. 10(c) is the composite image with JPEG format; Fig. 10(d) is the image components; Fig. 10(e) is the normalization of variances of remaining noise of image components; and Fig. 10(f) is the obtained result of tampering detection using the proposed method.

Table 1 shows the image formats of the target, source, and composite images in own dataset (Figs. 5–10). The proposed tampering detection method works well for both compressed (JPEG) and uncompressed (BMP) formats. Table 2 shows the results of the performance evaluation in own dataset. The proposed method has good composite image detection performance.

Experimental results show that the proposed method can work well for composite images whose target and source images are in either compressed or uncompressed format or a mixture, and for

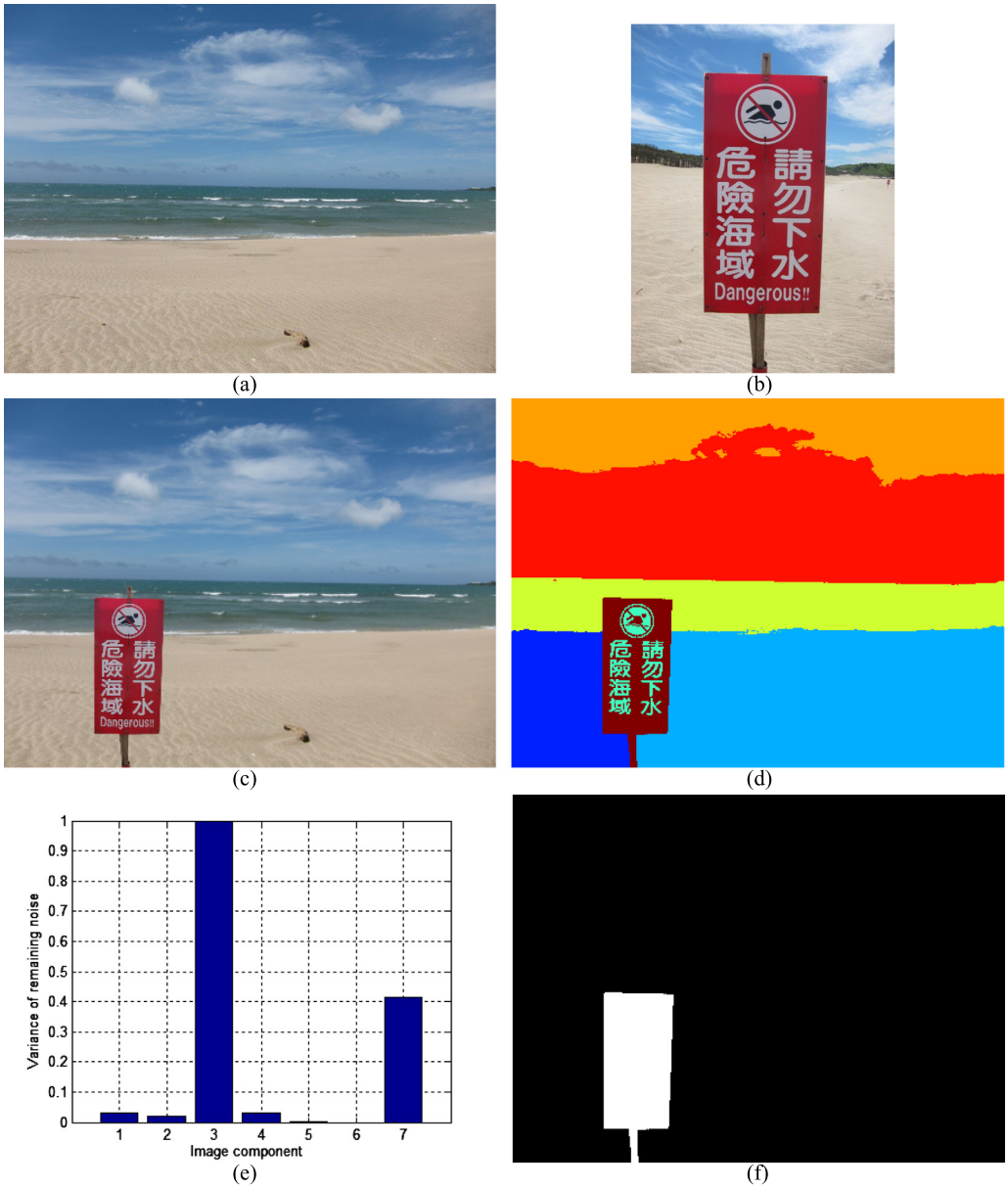


**Fig. 6.** Tampering detection of image of beach. (a) Target image, (b) source image, (c) composite image, (d) image components, (e) normalization of variances of remaining noise, and (f) detected tampered region.

**Table 1**
Image formats of target, source, and composite images in own dataset.

| | Target image | Source image | Composite image |
|---|---|---|---|
| Fig. 5 (Eagle image) | JPEG | JPEG | BMP |
| Fig. 6 (Beach image) | JPEG | BMP | BMP |
| Fig. 7 (Pyramid image) | JPEG | JPEG | JPEG |
| Fig. 8 (Sky image) | BMP | BMP | BMP |
| Fig. 9 (Highway image) | BMP | JPEG | JPEG |
| Fig. 10 (Butterfly image) | BMP | BMP | JPEG |

**Table 2**
Performance evaluation in own dataset.

| | Sensitivity $S_e$ | Specificity $S_p$ | Spatial accuracy $S_a$ |
|---|---|---|---|
| Fig. 5 (Eagle image) | 0.9491 | 0.9998 | 0.9418 |
| Fig. 6 (Beach image) | 0.9679 | 1.0 | 0.9679 |
| Fig. 7 (Pyramid image) | 0.9945 | 0.9957 | 0.9892 |
| Fig. 8 (Sky image) | 0.9770 | 0.9995 | 0.9539 |
| Fig. 9 (Highway image) | 0.9876 | 0.9998 | 0.9776 |
| Fig. 10 (Butterfly image) | 0.9856 | 0.9987 | 0.9203 |

tampered regions subjected to geometric operations (such as scaling, rotation, and morphing).

Compared to the tampering detection method based on local noise level inconsistency proposed by Mahdian and Saic [15], the method proposed here does not use additive Gaussian noise and works well as a standalone forgery detector for composite images.

Compared to the shadow-based tampering detection method proposed by Liu et al. [21], the method proposed here is not limited to a single distant light source and accurately determine which part of the composite image is doctored.

### 3.2. Performance evaluation in JPEG compression dataset

For evaluating the feasibility of proposed method under JPEG compression, an image dataset composed 50 images (highway and butterfly images in Figs. 9–10) saved with double JPEG compression was built (JPEG compression dataset). In this dataset, target image is JPEG compressed with a given quality factor $QF_1$, and composite image is JPEG compressed with a given quality factor

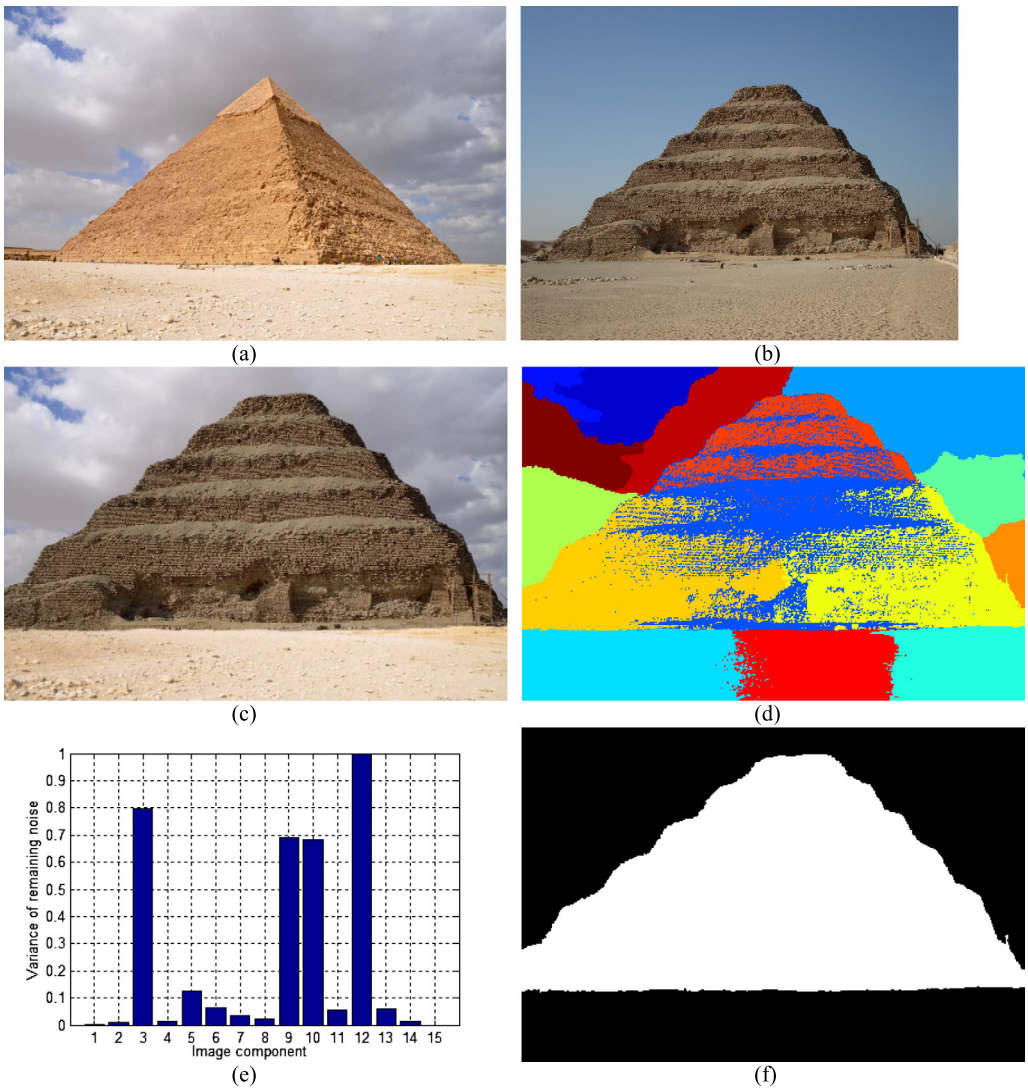


**Fig. 7.** Tampering detection of Pyramid image. (a) Target image, (b) source image, (c) composite image, (d) image components, (e) normalization of variances of remaining noise, and (f) detected tampered region.

**Table 3**
Spatial accuracy $S_a$ of highway images saved with double JPEG compression in JPEG compression dataset.

| $QF_1$ | $QF_2$ | | | | |
|---|---|---|---|---|---|
| | 50 | 60 | 70 | 80 | 90 |
| 50 | 0.9598 | 0.9612 | 0.9773 | 0.9706 | 0.9743 |
| 60 | 0.9794 | 0.9817 | 0.9772 | 0.9692 | 0.9844 |
| 70 | 0.9783 | 0.9711 | 0.9787 | 0.9744 | 0.9806 |
| 80 | 0.9827 | 0.9806 | 0.9832 | 0.9757 | 0.9759 |
| 90 | 0.9659 | 0.9717 | 0.9608 | 0.9620 | 0.9589 |

**Table 4**
Spatial accuracy $S_a$ of butterfly images saved with double JPEG compression in JPEG compression dataset.

| $QF_1$ | $QF_2$ | | | | |
|---|---|---|---|---|---|
| | 50 | 60 | 70 | 80 | 90 |
| 50 | 0.9200 | 0.9178 | 0.9221 | 0.9195 | 0.9471 |
| 60 | 0.9504 | 0.9487 | 0.9503 | 0.9568 | 0.9582 |
| 70 | 0.9514 | 0.9568 | 0.9582 | 0.9571 | 0.9496 |
| 80 | 0.9465 | 0.9500 | 0.9510 | 0.9455 | 0.9560 |
| 90 | 0.9416 | 0.9487 | 0.9579 | 0.9536 | 0.9779 |

$QF_2$, where $QF_1 = [50, 60, 70, 80, 90]$ and $QF_2 = [50, 60, 70, 80, 90]$. Tables 3–4 show the spatial accuracy $S_a$ of highway and butterfly images in JPEG compression dataset, respectively. The average spatial accuracy $S_a$ is 0.9601 in JPEG compression dataset. The average sensitivity $S_e$ is 0.9796 in JPEG compression dataset. The average specificity $S_p$ is 0.9997 in JPEG compression dataset. Experimental results were shown that the proposed tampering detection has good performance in the feasibility of JPEG compression.

Two state-of-the-art methods, JPEG-compression-based tampering detection method [20] and block posterior probability map (BPPM)-based tampering detection method [31], were used to compare with the proposed method to evaluate the performance in JPEG compression dataset.

JPEG-compression-based tampering detection method, proposed by Bianchi and Piva [20] was used to compare with the proposed method. The source code was downloaded from the author's website (http://lesc.det.unifi.it/en/node/187). Figs. 11(a) and 11(b) are the tampering detection of butterfly image saved with double JPEG compression ($QF_1 = 80, QF_2 = 90$) and ($QF_1 = 90, QF_2 = 50$) using JPEG-compression-based tampering detection method [20], respectively, where red/blue areas correspond to high/low probability of being doubly compressed and they can be further used to check tampered regions. The left side of Figs. 11(a) and 11(b) are the re-

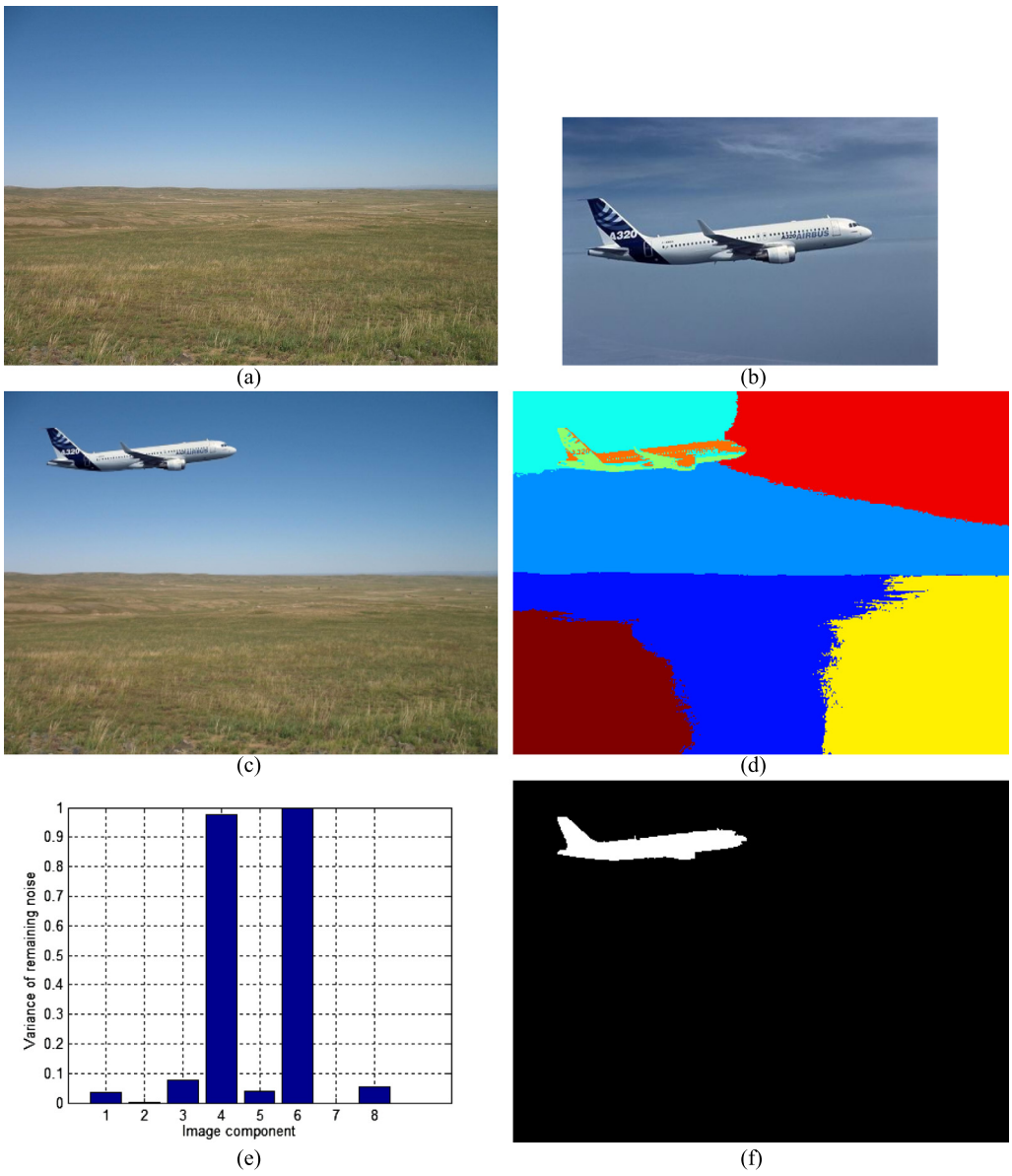


**Fig. 8.** Tampering detection of image with sky. (a) Target image, (b) source image, (c) composite image, (d) image components, (e) normalization of variances of remaining noise, and (f) detected tampered region.

sults using aligned double JPEG (A-DJPG) compression. The right side of Figs. 11(a) and 11(b) are the results using nonaligned double JPEG (NA-DJPG) compression. Experimental results show that the tampered regions are not accurately detected. Besides, the identification of tampered images needs to be decided manually by the user because the identification rule was not given in the literature [20]. Furthermore, based on authors' suggestion [20], their method is able to correctly identify traces of A-DJPG compression unless $QF_2 = QF_1$ or $QF_2 \ll QF_1$, and it is able to correctly identify traces of NA-DJPG compression whenever $QF_2 > QF_1$ and there is a sufficient percentage of doubly compressed blocks.

The detection accuracy of JPEG-compression-based tampering detection method [20] in JPEG compression dataset is 76% and 42% using A-DJPG compression and NA-DJPG compression, respectively, where detection accuracy is defined as accurate identification of tampered images.

In JPEG compression dataset, BPPM-based tampering detection method [31] makes tampering detection fail for all tampered images. Based on the author's (Prof. Zhouchen Lin) suggestion [31], three working conditions of BPPM-based tampering detection method are: (1) The unchanged region (un-tampered region) is from a JPEG image and its DCT grid does not change after tampering; (2) The quality of second JPEG compression is higher than that of the original JPEG of the unchanged region (that is, $QF_2 > QF_1$); and (3) The area of changed region (tampered region) should be moderate. If it is too large or too small, the DW effect is not salient. The ideal proportion of changed region should be within 30%–70% of the image. Because the tampered region is not within 30%–70% of the composite image in JPEG compression dataset, detection capability of BPPM-based tampering detection method is ineffective in JPEG compression dataset.

The computational complexity of A-DJPG compression [20], NA-DJPG compression [20], and BPPM-based method [31] are all $O(N)$, and the computational complexity of our method is $O(N^2)$, where $N$ is the total pixels of the tested image. The computational cost of our method is mainly spent on the adaptive component detection method. Because the adaptive component detection method needs to use mean shift algorithm and spectral segmentation with the $k$-means algorithm, the computational cost is high. It is worth mentioning that the computational complexity can be effectively

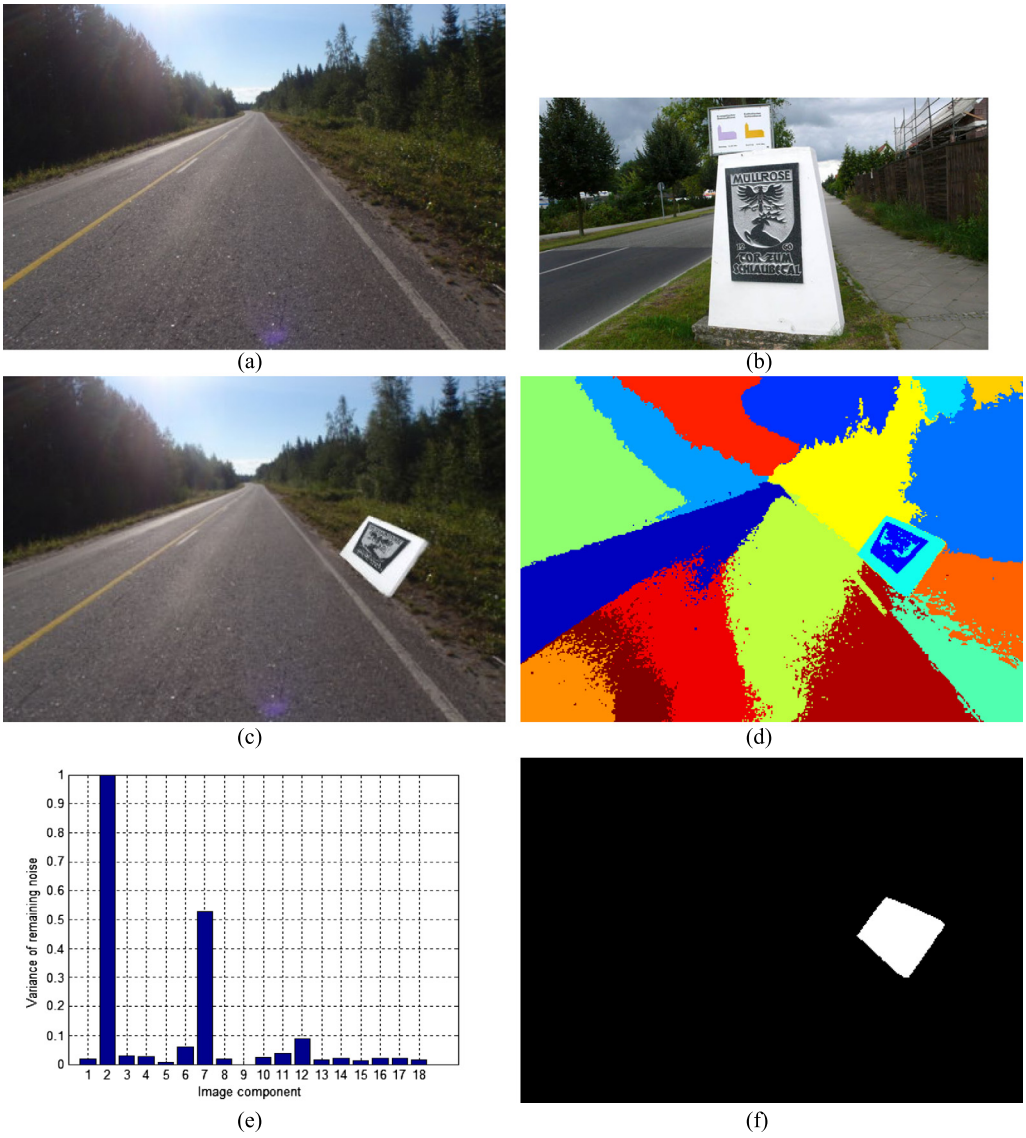


**Fig. 9.** Tampering detection of image with highway. (a) Target image, (b) source image, (c) composite image, (d) image components, (e) normalization of variances of remaining noise, and (f) detected tampered region.

reduced by the following solutions [32]: (1) clever choice of kernel supports (such as in the image segmentation examples), (2) introduction of approximate iterations (such as the Fast Gauss Transform [33]), (3) use of suitable stopping criteria to eliminate unnecessary iterations, and (4) employing other heuristic rules that save computations (such as checking conditions similar to the information force tree approach [34]). Therefore, the proposed method is feasibility for image tampering detection.

A-DJPG compression [20], NA-DJPG compression [20], and BPPM-based method [31] are all the non-overlapping blocks-based tampering detection methods and they would obtain tampered regions with jagged shapes. Our method uses image components rather than non-overlapping blocks, thus our method can obtain more fine contours of tampered regions than ones obtained using these non-overlapping blocks-based tampering detection methods.

Furthermore, A-DJPG compression [20], NA-DJPG compression [20], and BPPM-based method [31] make the tampering detection fail whenever the target image is not saved with JPEG format and only composite image is saved with JPEG format, such as the cases of Figs. 9 and 10.

Compared to JPEG-compression-based tampering detection methods [17–20,31], experimental results show that the proposed method can work well for without the limitation of quality factors in JPEG compression for target and composite images.

### 3.3. Performance evaluation in CASIA v1.0 dataset

An open source database-CASIA v1.0 dataset [30] is used to evaluate the performance of the proposed method. CASIA v1.0 dataset focus on splicing detection evaluation. Image splicing is defined as a simple cut-and-paste operation of image regions from one image onto the same or another image without performing post-processing. It is a fundamental operation of tampering. CASIA v1.0 dataset has 1721 images which contain 800 authentic and 921 spliced color images of size $384 \times 256$ pixels with JPEG format. Five state-of-the-art methods, JPEG-compression-based tampering detection method [20], BPPM-based method [31], SPN-based methods [23,35], and EXIF-noise-based tampering detection method [29], were used to compare with the proposed method to evaluate the performance in CASIA v1.0 dataset. Comparison of detection capability in CASIA v1.0 dataset is list in Table 5.

In CASIA v1.0 dataset, 98.96% of 1721 images don't have aperture, shutter speed and ISO in the EXIF headers, which are needed in EXIF-noise-based tampering detection method [29]. There-

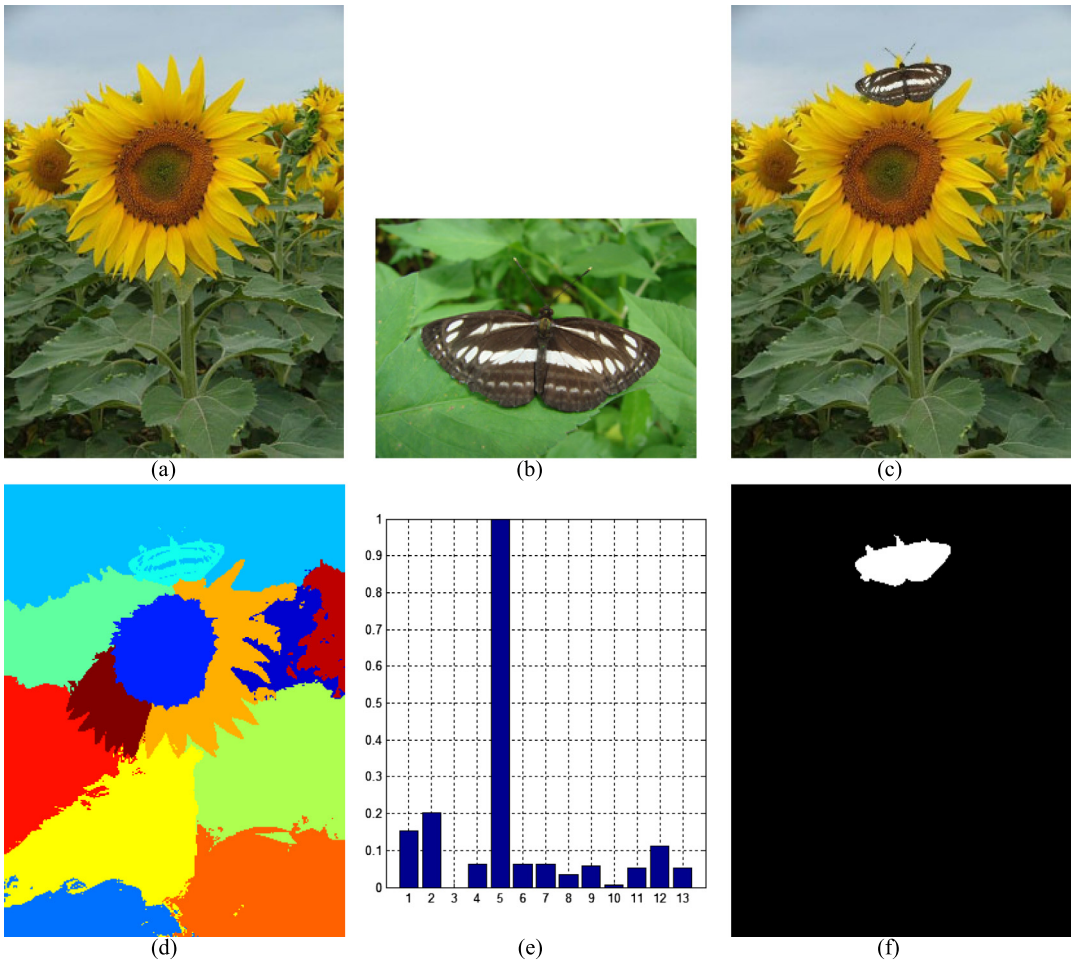


**Fig. 10.** Tampering detection of image with butterfly. (a) Target image, (b) source image, (c) composite image, (d) image components, (e) normalization of variances of remaining noise, and (f) detected tampered region.

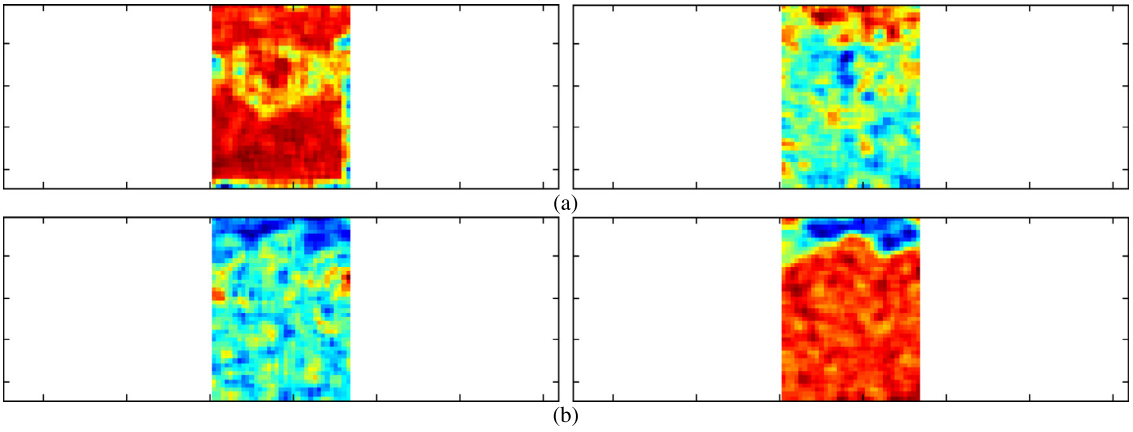


**Fig. 11.** Tampering detection of butterfly image (saved with double JPEG compression) using method proposed by Bianchi and Piva [20]. (a) ($QF_1 = 80, QF_2 = 90$), and (b) ($QF_1 = 90, QF_2 = 50$). (For interpretation of the colors in this figure, the reader is referred to the web version of this article.)

fore, detection capability of EXIF-noise-based tampering detection method is ineffective in CASIA v1.0 dataset.

In SPN-based method for camera identification [23], the correlation is calculated between the image noise residual and the known camera reference pattern to decide whether a tested image was taken by a specific camera, where camera reference pattern is an approximation of the pixel nonuniformity (PNU) noise. In SPN-based method for image tampering detection [35], the sliding block is used and then the correlation is calculated between the block noise residual and the known camera reference pattern to detect the tampered regions. In CASIA v1.0 dataset, all images don't know that were taken by the types of cameras. It is necessary to know camera reference pattern in SPN-based methods [23,35]. Therefore, detection capability of SPN-based methods [23, 35] is ineffective in CASIA v1.0 dataset. Besides, all images are also without camera reference pattern in own dataset and JPEG compression dataset, because these tested images were downloaded from Internet. Therefore, detection capability of SPN-based meth-

**Table 5**
Comparison of detection capability in CASIA v1.0 dataset.

| | JPEG-compression-based method [20] | EXIF-noise-based method [29] | BPPM-based method [31] | SPN-based methods [23,35] | Our method |
|---|---|---|---|---|---|
| CASIA v1.0 dataset | Effective | Ineffective | Effective | Ineffective | Effective |

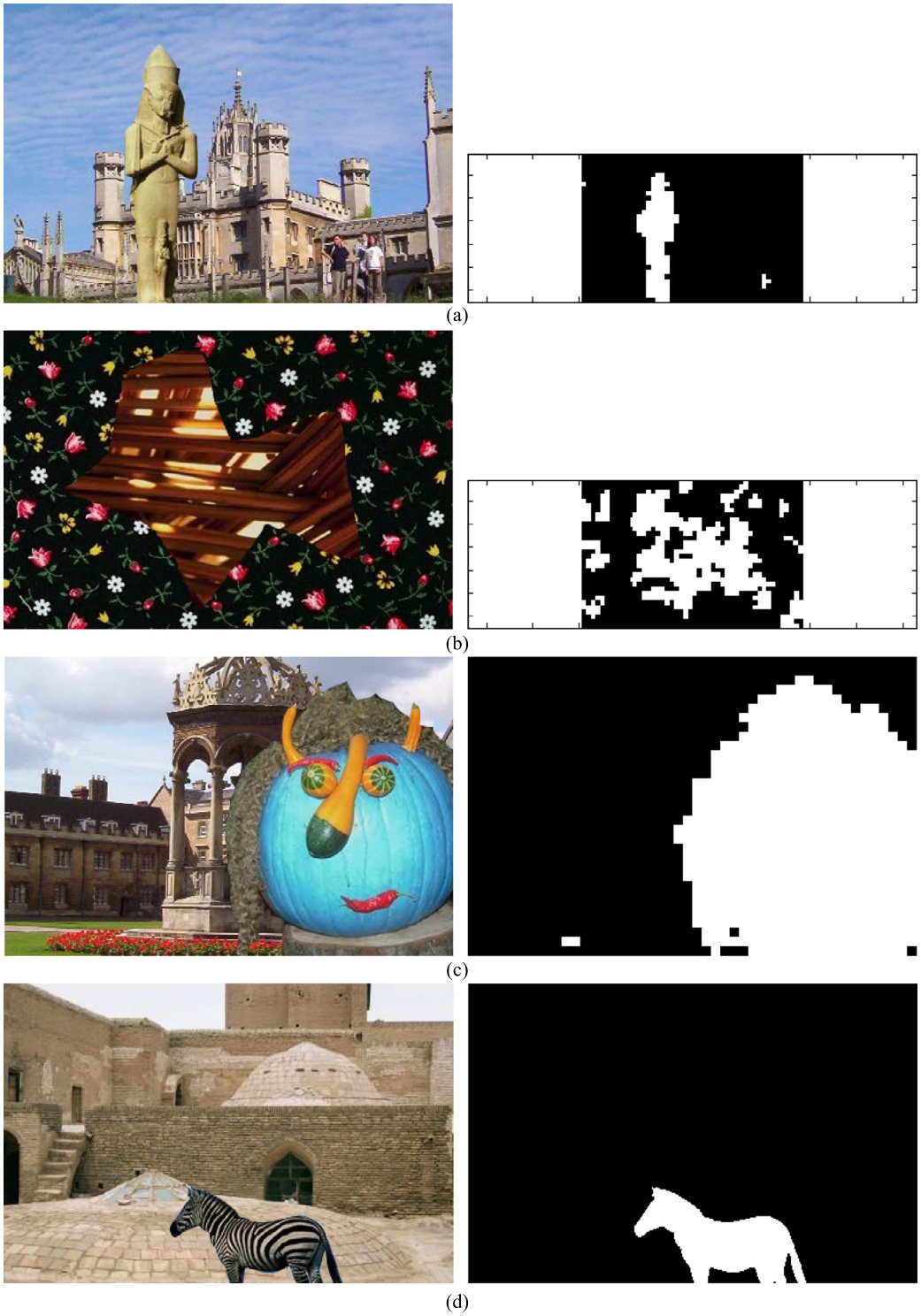


**Fig. 12.** Detected tampered regions of some examples in the selected CASIA v1.0 database. (a) Result using the A-DJPG compression, (b) result using the NA-DJPG compression, (c) result using the BPPM-based method, and (d) result using our method.

**Table 6**
Performance evaluation in selected CASIA v1.0 dataset.

| | A-DJPG compression [20] | NA-DJPG compression [20] | BPPM-based method [31] | Our method |
|---|---|---|---|---|
| $\overline{TP}$ | 179 | 150 | 77 | 127 |
| $\overline{TN}$ | 468 | 471 | 561 | 643 |
| $\overline{FP}$ | 332 | 329 | 239 | 157 |
| $\overline{FN}$ | 281 | 310 | 383 | 333 |

**Table 7**
Detection accuracy of authentic images and composite images in selected CASIA v1.0 dataset.

| | A-DJPG compression [20] | NA-DJPG compression [20] | BPPM-based method [31] | Our method |
|---|---|---|---|---|
| Authentic images | 58.50% | 58.88% | 70.13% | 80.38% |
| Composite images | 38.91% | 32.61% | 16.74% | 27.61% |

ods [23,35] is ineffective in own dataset and JPEG compression dataset.

Furthermore, 921 spliced images of CASIA v1.0 dataset have 461 images which belong to copy–move image forgery (simple cut-and-paste operation of image regions from one image onto the same image), thus there are only 460 composite images. Therefore, 1260 tested images (800 authentic and 460 composite images) are used to further evaluate the performance of JPEG-compression-based tampering detection [20] method, BPPM-based method [31], and our method. These 1260 tested images are named as the selected CASIA v1.0 dataset. Fig. 12 is the detected tampered regions of some examples in the selected CASIA v1.0 dataset, where Fig. 12(a) is the result using the A-DJPG compression [20], Fig. 12(b) is the result using the NA-DJPG compression [20], Fig. 12(c) is the result using the BPPM-based method [31], and Fig. 12(d) is the result using our method.

Table 6 is the performance evaluation results using A-DJPG compression [20], NA-DJPG compression [20], BPPM-based method [31], and our method in selected CASIA v1.0 dataset, where $\overline{TP}$ is the total number of true positive images, $\overline{FP}$ is the total number of false positive images, $\overline{TN}$ is the total number of true negative images, and $\overline{FN}$ is the total number of false negative images.

The detection accuracy of A-DJPG compression, NA-DJPG compression, BPPM-based method, and our method are 51.35%, 49.29%, 50.63, and 61.11%, respectively. The detection accuracy is defined in (10). Experimental results show that the proposed method outperforms state-of-the-art methods [20,31] for JPEG-compression tampering detection.

$$D_a = (\overline{TP} + \overline{TN})/(\overline{TP} + \overline{TN} + \overline{FP} + \overline{FN}) \tag{10}$$

Furthermore, the detection accuracy of authentic images and composite images using different methods can be further broken down as Table 7.

The reason of low detection accuracy using A-DJPG compression and NA-DJPG compression maybe is the given identification rule not being optimal. The low detection accuracy using BPPM-based method maybe is caused from the limitations of three working conditions of BPPM-based tampering detection method, which were reported in Subsection 3.2. The main reason of low detection accuracy using our method is that the obtained image components using the adaptive component detection method [10] are not the accurate result, because the adaptive component detection method is suitable for image segmentation of images having the foreground objects. It is worth mentioning that a more suitable detection method of image components can effectively raise the detection accuracy of our method.

## 4. Conclusion

This paper proposed an effective composite image detection method. The image components are first obtained using adaptive component detection. Next, the variance of the noise remaining after de-noising in each image component is calculated. Finally, the tampered regions are detected using the variance of the remaining noise of image components based on a tampering detection rule.

This paper makes three major contributions. (i) The proposed method uses image components rather than non-overlapping blocks to obtain fine contours of tampered regions. (ii) The variance of noise remaining after de-noising (sensor pattern noise) is used to determine feature inconsistency for tampering detection. (iii) The proposed method can work well for without the limitation of quality factors in image compression for target and composite images, for composite images whose target and source images are in either compressed or uncompressed format or a mixture, and for tampered regions subjected to geometric operations (such as scaling, rotation, and morphing). Experimental results show that the proposed method has good composite image detection performance and that it outperforms state-of-the-art methods for composite image detection. Therefore, the proposed method is a useful forgery detector for composite images.

## Acknowledgments

This work was supported by the National Science Council of Taiwan under grant NSC102-2221-E-346-007 and MOST103-2221-E-346-007. The authors wish to express the appreciation to Mr. Chu-Lin Chuang, Mrs. Jiayuan Fan, Prof. Alessandro Piva, Prof. Zhouchen Lin, and Prof. Wei Wang for their help with the experiments. The authors also gratefully acknowledge the helpful comments and suggestions of reviewers, which have improved the quality and presentation.

## References

[1] G.-S. Lin, M.-K. Chang, Y.-L. Chen, A passive-blind forgery detection scheme based on content-adaptive quantization table estimation, IEEE Trans. Circuits Syst. Video Technol. 21 (4) (2011) 421–434.
[2] G.K. Birajdar, V.H. Mankar, Digital image forgery detection using passive techniques: a survey, Digit. Investig. 10 (2013) 226–245.
[3] Z. Zhang, Z. Yu, B. Su, Detection of composite forged image, in: Proc. of the 2010 International Conference on Computer Application and System Modeling, vol. 7, 2010, pp. 572–576.
[4] K.-C. Liu, Colour image watermarking for tamper proofing and pattern-based recovery, IET Image Process. 6 (5) (2012) 445–454.
[5] W.-C. Hu, W.-H. Chen, Effective forgery detection using DCT+SVD-based watermarking for region of interest in key frames of vision-based surveillance, Int. J. Comput. Sci. Eng. 8 (4) (2013) 297–305.
[6] Q. Han, L. Han, E. Wang, J. Yang, Dual watermarking for image tamper detection and self-recovery, in: Proc. of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013, pp. 33–36.
[7] W.-C. Hu, W.-H. Chen, D.-Y. Huang, C.-Y. Yang, Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes, Multimed. Tools Appl. (2015), http://dx.doi.org/10.1007/s11042-015-2449-0.
[8] W.-C. Hu, W.-H. Chen, C.-Y. Yang, Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition, J. Electron. Imaging 21 (3) (2012) 033005.

[9] W.-C. Hu, J.-J. Jhu, C.-P. Lin, Unsupervised and reliable image matting based on modified spectral matting, J. Vis. Commun. Image Represent. 23 (4) (2012) 665–676.
[10] W.-C. Hu, J.-F. Hsu, Automatic spectral video matting, Pattern Recognit. 46 (4) (2013) 1183–1194.
[11] G. Lynch, F.Y. Shih, H.-Y.M. Liao, An efficient expanding block algorithm for image copy–move forgery detection, Inf. Sci. 239 (2013) 253–265.
[12] Y. Huang, W. Lu, W. Sun, D. Long, Improved DCT based detection of copy–move forgery in images, Forensic Sci. Int. 206 (1–3) (2011) 178–184.
[13] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, An evaluation of popular copy–move forgery detection approaches, IEEE Trans. Inf. Forensics Secur. 7 (6) (2012) 1841–1854.
[14] L. Li, S. Li, H. Zhu, S.-C. Chu, J.F. Roddick, J.-S. Pan, An efficient scheme for detecting copy–move forged images by local binary patterns, J. Inf. Hiding Multimed. Signal Process. 4 (1) (2013) 46–56.
[15] B. Mahdian, S. Saic, Using noise inconsistencies for blind image forensics, Image Vis. Comput. 27 (10) (2009) 1497–1503.
[16] A.C. Popescu, Statistical tools for digital image forensics, Ph.D. Dissertation, Department of Computer Science, Dartmouth College, Hanover, NH, 2005.
[17] J.-X. Zuo, S.-J. Pan, B.-Y. Liu, X. Liao, Tampering detection for composite images based on re-sampling and JPEG compression, in: Proc. of the First Asian Conference on Pattern Recognition, 2011, pp. 169–173.
[18] H. Farid, Exposing digital forgeries from JPEG ghosts, IEEE Trans. Inf. Forensics Secur. 4 (1) (2009) 154–160.
[19] E.-G. Zheng, X.-J. Ping, Passive-blind forensics for a class of JPEG image forgery, J. Electron. Inf. Technol. 32 (2) (2010) 394–399.
[20] T. Bianchi, A. Piva, Image forgery localization via block-grained analysis of JPEG artifacts, IEEE Trans. Inf. Forensics Secur. 7 (3) (2012) 1003–1017.
[21] Q. Liu, X. Cao, C. Deng, X. Guo, Identifying image composites through shadow matte consistency, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1111–1122.
[22] I.-C. Chang, J.C. Yu, C.-C. Chang, A forgery detection algorithm for exemplar-based inpainting images using multi-region relation, Image Vis. Comput. 31 (1) (2013) 57–71.
[23] J. Lukáš, J. Fridrich, M. Goljan, Digital camera identification from sensor pattern noise, IEEE Trans. Inf. Forensics Secur. 1 (2) (2006) 205–214.
[24] D. Comaniciu, P. Meer, Mean shift: a robust approach toward feature space analysis, IEEE Trans. Pattern Anal. Mach. Intell. 24 (5) (2002) 603–619.
[25] A. Levin, A. Rav-Acha, D. Lischinski, Spectral matting, IEEE Trans. Pattern Anal. Mach. Intell. 30 (10) (2008) 1699–1712.
[26] R.C. Hardie, C.G. Boncelet, LUM filters: a class of rank-order-based filters for smoothing and sharpening, IEEE Trans. Signal Process. 41 (3) (1993) 1061–1076.
[27] W.-C. Hu, C.-Y. Yang, D.-Y. Huang, Robust real-time ship detection and tracking for visual surveillance of cage aquaculture, J. Vis. Commun. Image Represent. 22 (6) (2011) 543–556.
[28] E.J. Carmona, J. Martínez-Cantos, J. Mira, A new video segmentation method of moving objects based on blob-level knowledge, Pattern Recognit. Lett. 29 (3) (2008) 272–285.
[29] J. Fan, H. Cao, A.C. Kot, Estimating EXIF parameters based on noise features for image manipulation detection, IEEE Trans. Inf. Forensics Secur. 8 (4) (2013) 608–618.
[30] CASIA image tampering detection evaluation database, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science [Online]. Available: http://forensics.idealtest.org.
[31] Z. Lin, J. He, X. Tang, C.K. Tang, Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis, Pattern Recognit. 42 (11) (2009) 2492–2501.
[32] U. Ozertem, D. Erdogmus, R. Jenssen, Mean shift spectral clustering, Pattern Recognit. 41 (6) (2008) 1924–1938.
[33] L. Greengard, J. Strain, The fast Gauss transform, SIAM J. Sci. Stat. Comput. 12 (1) (1991) 79–94.
[34] R. Jenssen, D. Erdogmus, K.E. Hild II, J.C. Principe, T. Eltoft, Information force clustering using directed trees, in: Proc. of 2003 Conference on Computer Vision and Pattern Recognition, 2003, pp. 68–72.
[35] M. Chen, J. Fridrich, M. Goljan, J. Lukáš, Determining image origin and integrity using sensor noise, IEEE Trans. Inf. Forensics Secur. 3 (1) (2008) 74–90.

**Wu-Chih Hu** received his Ph.D. degree in electrical engineering from the National Taiwan University of Science and Technology, Taiwan, in 1998. From 1998, he worked at the National Penghu University of Science and Technology for 16 years. He is currently the chairman and Professor in the Department of Computer Science and Information Engineering. He has published more than 100 papers in journal and conference proceedings since 1998. He obtained the Best Paper Awards of ICGEC2010, RVSP2011, ACIIDS2012, ISIC2012, and ICGEC2013. His current research interests include computer vision, image processing, pattern recognition, digital watermarking, visual surveillance, and video processing.

**Jing-Siou Dai** received his University degree in computer science and information engineering from the National Penghu University of Science and Technology, Taiwan, in 2013. His recent research interests include image processing and pattern recognition.

**Jhih-Syuan Jian** received his University degree in computer science and information engineering from the National Penghu University of Science and Technology, Taiwan, in 2013. He now studies MS degree in Department of Graduate Institute of Electrical Engineering and Computer Science, National Penghu University of Science and Technology, Taiwan. His recent research interests include image processing and video processing.