Detecting Copy-move Forgeries in Images Based on DCT and Main Transfer Vectors

Zhi Zhang[#], Dongyan Wang[#], Chengyou Wang*, and Xiao Zhou
School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China
[e-mail: zhi@mail.sdu.edu.cn, wdy@mail.sdu.edu.cn, wangchengyou@sdu.edu.cn, zhouxiao@sdu.edu.cn]
[#]These authors are co-first authors and contributed equally to this work.
*Corresponding author: Chengyou Wang

Received January 23, 2017; revised April 17, 2017; accepted May 26, 2017;
published September 30, 2017

Abstract

With the growth of the Internet and the extensive applications of image editing software, it has become easier to manipulate digital images without leaving obvious traces. Copy-move is one of the most common techniques for image forgery. Image blind forensics is an effective technique for detecting tampered images. This paper proposes an improved copy-move forgery detection method based on the discrete cosine transform (DCT). The quantized DCT coefficients, which are feature representations of image blocks, are truncated using a truncation factor to reduce the feature dimensions. A method for judging whether two image blocks are similar is proposed to improve the accuracy of similarity judgments. The main transfer vectors whose frequencies exceed a threshold are found to locate the copied and pasted regions in forged images. Several experiments are conducted to test the practicability of the proposed algorithm using images from copy-move databases and to evaluate its robustness against post-processing methods such as additive white Gaussian noise (AWGN), Gaussian blurring, and JPEG compression. The results of experiments show that the proposed scheme effectively detects both copied region and pasted region of forged images and that it is robust to the post-processing methods mentioned above.

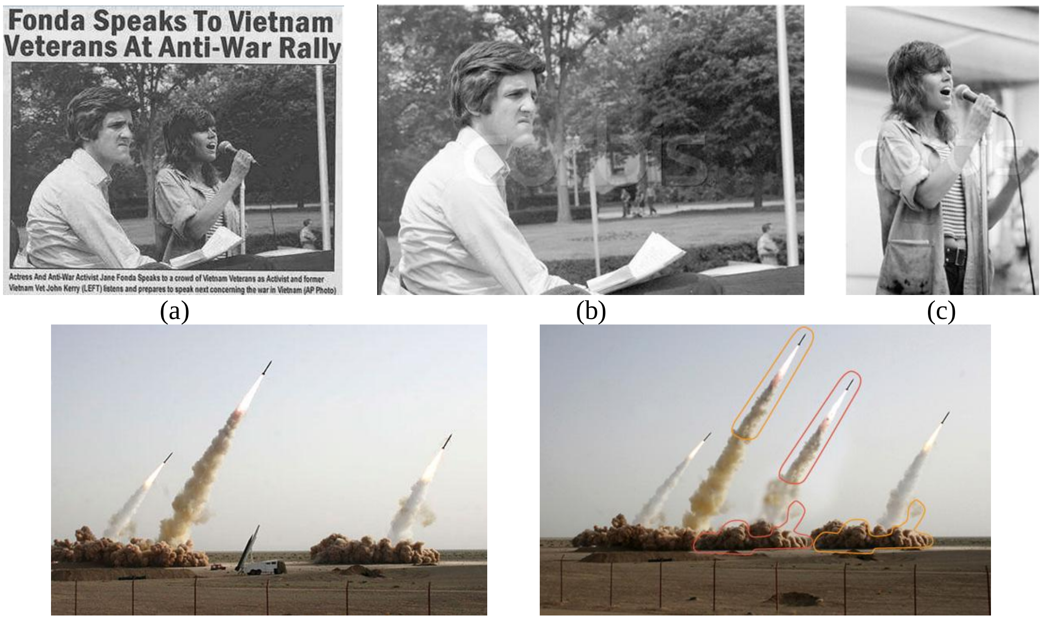
Keywords: Image tamper detection, copy-move forgery detection, discrete cosine transform (DCT), main transfer vector, lexicographical sort

This work was supported by the National Natural Science Foundation of China (No. 61702303, No. 61201371), the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022), and the Natural Science Foundation of Shandong Province, China (No. ZR2017MF020, No. ZR2015PF004). Zhi Zhang, Dongyan Wang, and Chengyou Wang conceived the algorithm; Zhi Zhang and Dongyan Wang designed and performed the experiments; Chengyou Wang and Xiao Zhou analyzed the results; Dongyan Wang drafted the manuscript; Zhi Zhang and Dongyan Wang revised the manuscript; Chengyou Wang and Xiao Zhou supervised the research project.

https://doi.org/10.3837/tiis.2017.09.021 **ISSN : 1976-7277**

1. Introduction

With the rapid development of the Internet and improved manufacturing techniques for precision instruments, people spend less time downloading large multimedia files from servers to local devices. Moreover, it is becoming increasingly convenient to acquire information from the natural world and it has been unfolded visually for people in the form of high-quality multimedia. However, along with the improvement of image editing softwares available on the Internet, there has been an increase of images that have been tampered without leaving obvious traces. Undetected forged images have a malign influence on the international community [1]. Two actual events from history are provided in **Fig. 1**. **Fig. 1(a)** shows Senator John Kerry and Jane Fonda sharing a stage at an antiwar rally during the 2004 Presidential primary when Senator John Kerry was pursuing the Democratic nomination [2]. However, the image of Senator John Kerry was taken in June 1971, while the picture of Jane Fonda was taken in August 1972. In other words, **Fig. 1(a)** is not a photograph but a composited image. **Fig. 1(d)** shows an actual Iranian missile test situation, while **Fig. 1(e)** [3] shows the published version, in which the third missile from the left was digitally added to the image to cover up a missile on the ground that did not fire.


Fonda Speaks To Vietnam Veterans At Anti-War Rally
Actress And Anti-War Activist Jane Fonda Speaks to a crowd of Vietnam Veterans as Activist and former Vietnam Vet John Kerry (LEFT) listens and prepares to speak next concerning the war in Vietnam (AP Photo)

(a) (b) (c)

(d) (e)

Fig. 1. Actual doctored images from historical events: (a) Senator John Kerry and Jane Fonda sharing a stage at an antiwar rally (2004), (b) Picture Senator John Kerry (1971), (c) Picture Jane Fonda (1972), (d) the real Iranian missile test situation, and (e) the doctored published Iranian missile test image.

Digital image forensics is a technique to verify the integrity and authenticity of image content. There are two types: active forensics and passive forensics. Active forensics refers that preprocessing operations are performed on the original content, for example, embedding authentication information into carriers in advance. Currently, such techniques primarily involve digital watermarking technology [4] and digital signature technology [5]. By verifying the integrity of embedded authentication information, a recipient can know whether the image has been tampered. However, this type of technique requires special softwares or hardwares to insert the authentication information into images before they are distributed. In contrast, passive tamper detection techniques use only the relevant characteristics of received images to examine whether they have been tampered. No watermark or signature is required in the original content.

There are many types of image tampering approaches, including recompression, copy-move, fuzzy retouching, resampling, etc. Copy-move is one of the most common techniques used for image forgery. Copy-move forgeries can be also classified into two categories: those in which the copied and pasted regions are sourced from different images (**Fig. 1(a)**) and those in which the copied and pasted regions are sourced from the same image (**Fig. 1(e)**). The latter type is typically used to either hide or replicate an object by copying and pasting an area over another region in the same image. Since the advent of this technique, numerous copy-move tamper detection algorithms have been proposed and implemented by researchers over the past several decades. Copy-move algorithms can be divided into two main classes: block-based methods and keypoint-based methods. After exhaustive search analysis, Fridrich *et al*. [6] first proposed a block-matching copy-move forgery detection method based on the discrete cosine transform (DCT). This scheme is a milepost of copy-move forgery detection. Popescu and Farid [7] proposed a scheme based on block-matching that used principal component analysis (PCA) rather than quantized DCT coefficients. Kang and Wei [8] used the singular values obtained through performing singular value decomposition (SVD) on the reduced-rank approximation of image blocks to realize copy-move detection. Zhao and Guo [9] combined DCT and SVD to propose a passive forensics scheme. Although the block-based methods mentioned above are accurate, they carry a high computational burden. Huang *et al*. [10] improved Fridrich's method [6] and ameliorated the computational complexity while maintaining detection accuracy. Bayram *et al*. [11] proposed a forgery detection scheme for copy-move based on the Fourier-Mellin transform (FMT), which is scale and rotation invariant. Amerini *et al*. [12] presented a copy-move counter-forensics technique based on the scale-invariant feature transform (SIFT) that could detect rough copied and pasted regions. Xu *et al*. [13] proposed a copy-move scheme based on speed up robust features (SURF) descriptors, which are keypoint features better than SIFT at matching in the presence of brightness variations and blurring. Pandey *et al*. [14] combined SURF, histogram oriented gradient (HOG), and SIFT features to come up with a passive copy-move forgery detection scheme. However, the keypoint-based methods mentioned above exhibit a visual output problem for the reason that the copied and pasted regions consist of lines and points which cannot present a clear and intuitive visual effect. Other copy-move image forgery detection schemes use features applied successfully in other disciplines to locate the duplicated regions. For example, Mahdian and Saic [15] adopted blur moment invariants of image blocks as the features for determining duplicated regions. This technique is robust to lossy JPEG compression. Malviya and Ladhake [16] proposed an image forensic technique for copy-move forgery detection, which employs the auto color correlogram, a tool successfully applied in image retrieval, to detect tampered region. Yang *et al*. [17] presented a copy-move scheme that combines the KAZE and SIFT features to detect modified region effectively. In [18], Vaishnavi and Subashini used contrast context histogram (CCH) features to detect duplicated regions in forged images.

In this paper, an improved copy-move forgery detection scheme is proposed that improves the process for judging the similarity between two image blocks. In addition, to reduce the feature dimensions, the sequence obtained by performing zig-zag scanning on quantized DCT coefficients is truncated using a truncation factor. After counting the frequencies of transfer vectors, this method finds the main transfer vectors whose frequencies exceed a threshold and uses them to locate the duplicated regions in forged images based on the top-left coordinates of the image blocks. Several experiments are conducted to verify its effectiveness and robustness. The results demonstrate that the proposed algorithm is both effective and robust.

The remaining sections of this paper are organized as follows. In Section 2, we review previous works that address copy-move forgery within the same image. Section 3 presents an improved copy-move forgery detection scheme in the DCT domain. Experimental results and analysis are presented in Section 4. Finally, Section 5 provides conclusions and discusses possible future work.

2. Related Works

2.1 Problem Analysis and Hypothesis

Based on the characteristics of copy-move forgery within the same image, the important theoretical basis for determining whether an image is tampered involves determining whether one or more similar parts of a certain area exist in the image. In [19], after studying numerous natural images, Luo *et al*. found that it is extremely rare to find images with areas containing two similar regions larger than 0.85% of the image itself. Following that reasoning, the algorithm proposed in this paper is based on the following assumptions:

(i) copied and pasted parts are disjoint in tampered images;

(ii) copied and pasted parts all consist of single connected regions whose area is larger than or equal to 0.85% of the tampered region;

(iii) the copied area has not been processed using any operation before pasting;

(iv) the tampered image may have been processed using post-processing methods.

The most direct method used to search for similar regions in the forged image is ergodic matching at the pixel level. However, the time complexity of such method is $O((MN)^2)$ when the image size is $M \times N$, which is not acceptable. However, it does not mean that all the copy-move forged regions can be accurately identified when traversing the image to find all the similar image blocks. Consequently, after finding the similar image blocks, it is necessary to eliminate false matching blocks.

2.2 General Algorithm Scheme

A generalized scheme for block-based copy-move forgery detection algorithms is summarized in **Fig. 2** and described below.

Step 1. Image segmentation. The input image is divided into image blocks;

Step 2. Feature representation. A proper feature vector is found that uniquely represents the corresponding image block;

Step 3. Traversal match. All image blocks are traversed to determine all the similar blocks;

Step 4. Tamper detection. All the similar blocks are examined to determine whether they meet the requirements that indicate tampering;

Step 5. Visual output. The final results should be output intuitively.

Note: Most current block-based copy-move forgery detection methods correspond to this common framework.

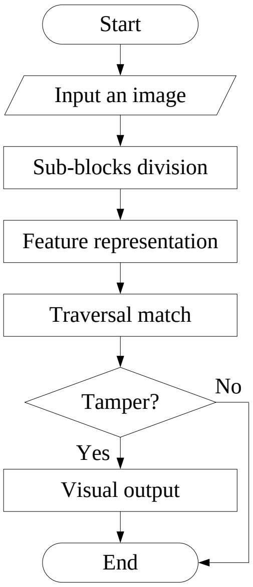


Fig. 2. Generalized scheme of block-based copy-move forgery detection algorithms.

3. Improved Copy-move Forgery Detection in the DCT Domain

In this section, we propose an improved copy-move forgery detection scheme based on the scheme first presented by Fridrich *et al.* in [6]. First, the DCT coefficients are quantized by a quantization factor instead of the standard JPEG quantization table. Then, the sequence obtained by performing zig-zag scanning on the quantized DCT coefficients is truncated using a truncation factor. False blocks matches are then excluded using specific rules. The feature extraction, feature matching, and algorithm processes are presented in detail.

3.1 Image Block and DCT Feature Extraction

In this paper, the block processing method is similar to that proposed by Fridrich *et al.* in [6]. The size of the image to be detected is $M \times N$. If the image is a color image, the luminance channel components of the image are extracted, and the image is transformed into a grayscale image using the formula: $I = 0.299R + 0.587G + 0.114B$, where R, G, and B are three channels of color images in RGB color model. Subsequently, moving from top to bottom and from left to right, a sliding block with size of $b \times b$ starts from the top-left of the image and slides one pixel at a time, finally obtaining $(M-b+1)(N-b+1)$ overlapping image blocks.

The DCT coefficients of the image blocks are extracted as the feature vectors of the corresponding blocks. For a digital image f whose size is $M \times N$, the DCT and inverse DCT transforms are shown in Eq. (1) and Eq. (2), respectively:

$$F(u,v) = \frac{2}{\sqrt{MN}} C(u)C(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[f(x,y) \cos\frac{(2x+1)u\pi}{2M} \cos\frac{(2y+1)v\pi}{2N} \right], \quad (1)$$

$$f(x,y) = \frac{2}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \left[C(u)C(v)F(u,v) \cos\frac{(2x+1)u\pi}{2M} \cos\frac{(2y+1)v\pi}{2N} \right], \quad (2)$$

In the above transforms, $u, x = 0, 1, \cdots, M-1$, $v, y = 0, 1, \cdots, N-1$, and

$$C(u),\ C(v) = \begin{cases} 1/\sqrt{2}, & u,v=0, \\ 1, & \text{otherwise.} \end{cases} \tag{3}$$

DCT can remove redundancy among adjacent pixels quickly and effectively, and it has energy compaction properties [20]. It is reasonable to adopt the DCT coefficients as features of image blocks. To reduce the dimensions and improve the efficiency of the matching process, the DCT coefficients are quantized by a quantization factor f_{q} rather than by the JPEG quantization table [6] and rounded to the nearest integer using Eq. (4):

$$\vec{a}_i = \left(\left[\frac{a_{i1}}{f_{\mathrm{q}}} \right], \left[\frac{a_{i2}}{f_{\mathrm{q}}} \right], \cdots, \left[\frac{a_{ik}}{f_{\mathrm{q}}} \right] \right),\ k = [f_{\mathrm{t}} \cdot b^2], \tag{4}$$

where $\vec{a}_i$ represents the feature vector of an image block.

Finally, the quantized DCT coefficients are converted into a row sequence using zig-zag scanning in the direction of the arrows shown in Fig. 3. The sequence is truncated by a truncation factor $f_{\mathrm{t}}(0 < f_{\mathrm{t}} < 1)$, in Eq. (4), which can be regarded as the feature representation of an image block.

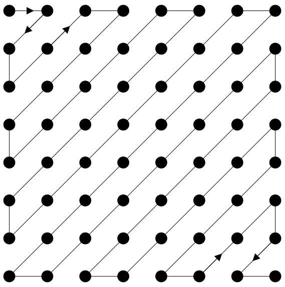


Fig. 3. Zig-zag scanning diagram.

3.2 Feature Matching

A lexicographic sort is used to build a feature matrix composed of the quantized DCT coefficients from each image block. The sorted results are stored in a matrix $\boldsymbol{A}$, and each row vector $\vec{a}_i$ in the matrix $\boldsymbol{A}$ should be matched with N_{a} adjacent row vectors. If the image is attacked using techniques such as compression, noise, and blurring, the feature vector of the copied image block and the feature vector of the pasted image block might simply be similar rather than identical. Therefore, some methods are required that can judge whether the corresponding feature vectors of the image blocks are the same. If the corresponding components of the two image blocks' vectors are nearly equal, the two image blocks can be considered as closely related. Here, the method that judges the similarity of the corresponding feature vectors of two image blocks is improved based on how the method in [10] determines that two image blocks are not the same when they do not meet the constraint condition. This approach may miss some similar image blocks. In order to solve the problem, the threshold c_{t} is introduced here, and an example is given below.

Here, we present an example used to illustrate the process of judging whether the feature vectors corresponding to two image blocks are the same. This also involves judging whether $\vec{a}_i = (a_i^1, a_i^2, \cdots, a_i^k)$ is the same as $\vec{a}_j = (a_j^1, a_j^2, \cdots, a_j^k)$. Where the thresholds s_{t} and t_{t} are predefined, $r_{\max}$ is initialized to a sufficiently small number, and $r_{\min}$ is initialized to a sufficiently large number, which are introduced for searching the similar image blocks. The counter c is initialized to 0; then, the specific judgment process is as follows. For each $1 \le l \le k$, if $a_j^l = 0$, we must determine whether it satisfies $|a_i^l - a_j^l| < s_t$. When it is satisfied, c is kept unchanged; otherwise, increment c by 1. If $a_j^l \ne 0$, calculate $r_l = a_i^l / a_j^l$ and correspondingly change the values $r_{\max}$ and $r_{\min}$: if $r_{\max} < r_l$, $r_{\max} = r_l$; if $r_{\min} > r_l$, $r_{\min} = r_l$. Eventually, this process will determine whether $r_{\max} - r_{\min} > t_t$ is satisfied. When it is satisfied, increment c by 1; otherwise, c is kept unchanged. Finally, if $c < c_t$, $\vec{a}_i$ and $\vec{a}_j$ are the same.

3.3 Algorithmic Process

The detailed processes of the improved copy-move forgery detection algorithm based on DCT are as follows:

Step 1. Set the digital image $\boldsymbol{I}$ to be detected as a grayscale image with size of $M \times N$;

Step 2. Set the size of the sliding block as $b \times b$. Let it slide by one pixel unit starting from the top-left corner of the image $\boldsymbol{I}$ and moving to the bottom-right corner. This process will obtain $(M-b+1)(N-b+1)$ image blocks;

Step 3. First, perform DCT on each image block. Second, use the quantization factor f_q to quantize the DCT coefficients. Third, convert the quantized DCT coefficients into a row sequence by zig-zag scanning and truncate it, as shown in Eq. (4). Finally, feature vectors of length $[f_t \cdot b^2]$ corresponding to each image block are obtained. All the image blocks' vectors are saved in a matrix $\boldsymbol{C}$;

Step 4. The matrix $\boldsymbol{A}$ is obtained by lexicographic sorting matrix $\boldsymbol{C}$; its size is $(M-b+1)(N-b+1) \times [f_t \cdot b^2]$;

Step 5. In matrix $\boldsymbol{A}$, each row vector $\vec{a}_i$ needs to be compared with its adjacent N_a row vectors $\vec{a}_j$, where N_a should satisfy: $j - i < N_a$;

Step 6. After judging whether the row vector $\vec{a}_i$ (top-left coordinate of image block is (x_1, y_1)) and the row vector $\vec{a}_j$ (top-left coordinate of image block is (x_2, y_2)) are roughly the same, calculate the transfer vector $\vec{s}$ between the two vectors, $\vec{s} = (s_1, s_2) = (x_1 - x_2, y_1 - y_2)$. If the distance $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} > T_d$, the transfer vector's existing frequency is incremented by 1;

Step 7. Find the main transfer vector whose frequencies exceed a threshold T_F. Any corresponding image blocks that are different from the main transfer vector is moved, and the remaining image blocks can be regarded as copied and pasted regions. When no main vector exists, the image under detection is not tampered; otherwise, continue with Step 8;

Step 8. The copied and pasted regions of the image are marked, respectively. Morphological processing is used to eliminate the isolated regions. After processing, the visualized image is the output.

4. Experimental Results and Analysis

In this section, we present the experimental processes, provide the related parameters, and report some of the experimental results. Finally, the accuracy, time complexity, and robustness of the proposed algorithm are analyzed through tables and figures.

4.1 Experimental Environment and Parameter Settings

All the experiments in this paper are conducted using MATLAB R2014a and a computer with an Intel Core 3.50 GHz processor. All the images used in the experiments are from the Columbia image-splicing detection evaluation dataset built by Ng and Chang [21], which is intended for testing digital image forensics, or from CoMoFoD, a database for copy-move forgery detection built by Tralic *et al.* [22]. In the experiments described below, the parameters values are set as follows: $b = 8$, $f_{\mathrm{t}} = 1/4$, $N_{\mathrm{a}} = 3$, $s_{\mathrm{t}} = 4$, $t_{\mathrm{t}} = 0.06$, $c_{\mathrm{t}} = 3$, $f_{\mathrm{q}} = 4$, $T_{\mathrm{F}} = 50$, and $T_{\mathrm{d}} = 20$. The parameter settings for the compared methods in [6, 8-10] are set as follows: $B = 16$ and $T = 80$ in [6]; $B = 20$, $S = 0.05$, $\rho = 24$, and $\varepsilon = 0.975$ in [8]; $b = 8$, $T_{\mathrm{d}} = 40$, and $T_{\mathrm{shift}} = 90$ in [9]; and $B = 8$, $T = 35$, $N_{\mathrm{f}} = 3$, $N_{\mathrm{d}} = 16$, $p = 0.25$, $q = 4$, $s\_threshold = 4$, and $t\_threshold = 0.0625$ in [10].

4.2 Performance Evaluation

To evaluate the performance of the proposed algorithm, we assess it from two aspects: the image level and the pixel level. At the image level, we emphasize the correct identification of tampered images. At the pixel level, we evaluate the proposed method based on how accurately it identifies the tampered region.

At the image level, we use the precision rate R_{P} and the recall rate R_{R} [23], which are defined in Eq. (5) and Eq. (6), respectively:

$$R_{\mathrm{P}} = \frac{N_{\mathrm{FF}}}{N_{\mathrm{FF}} + N_{\mathrm{IF}}}, \tag{5}$$

$$R_{\mathrm{R}} = \frac{N_{\mathrm{FF}}}{N_{\mathrm{FF}} + N_{\mathrm{FI}}}, \tag{6}$$

where N_{FF} is the number of forged images correctly detected as forged images, N_{IF} is the number of intact images erroneously detected as forged images, and N_{FI} is the number of forged images erroneously detected as intact images.

At the pixel level, we employ two criteria to evaluate the performance of the proposed method: detection accuracy rate (DAR) R_{DA} and false positive rate (FPR) R_{FP} [9] given by Eq. (7) and Eq. (8), respectively:

$$R_{\mathrm{DA}} = \frac{|\psi_{\mathrm{C}} \cap \tilde{\psi}_{\mathrm{DC}}| + |\psi_{\mathrm{P}} \cap \tilde{\psi}_{\mathrm{DP}}|}{|\psi_{\mathrm{C}}| + |\psi_{\mathrm{P}}|}, \tag{7}$$

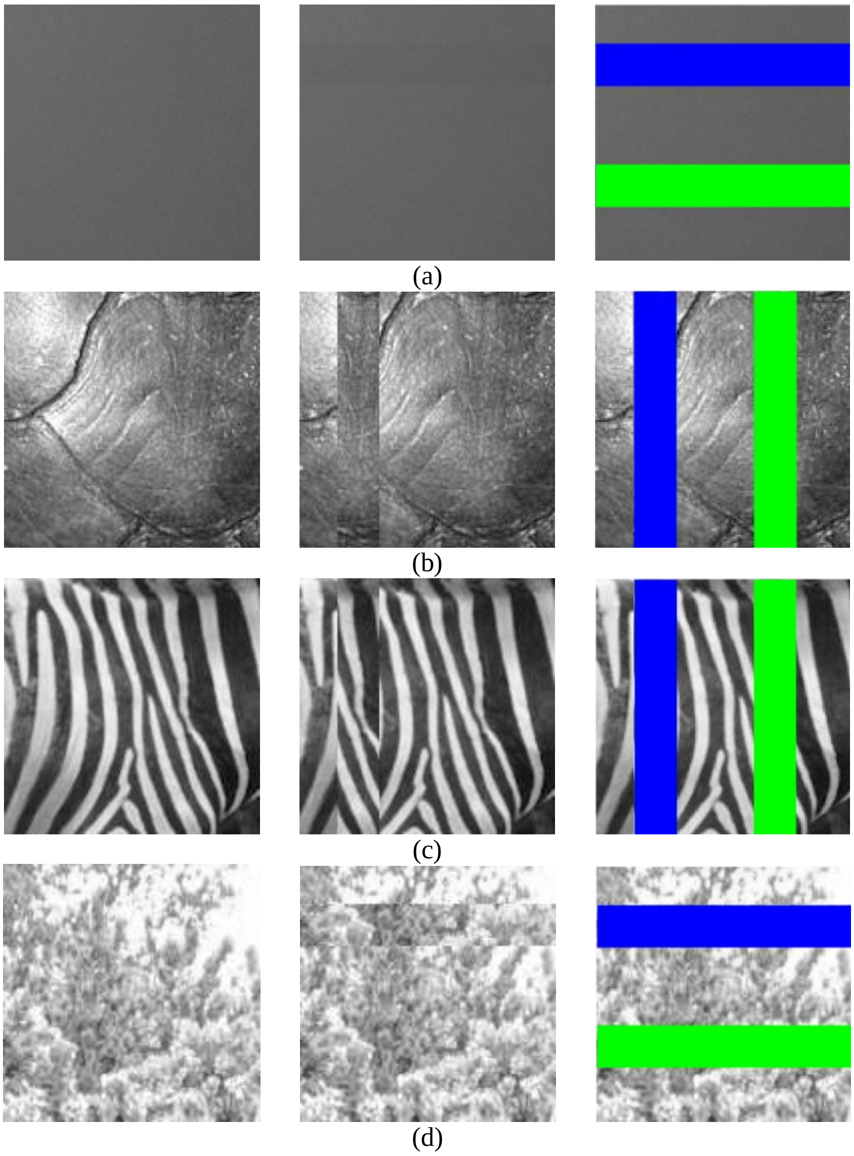
$$R_{\mathrm{FP}} = \frac{|\tilde{\psi}_{\mathrm{DC}} - \psi_{\mathrm{C}}| + |\tilde{\psi}_{\mathrm{DP}} - \psi_{\mathrm{P}}|}{|\tilde{\psi}_{\mathrm{DC}}| + |\tilde{\psi}_{\mathrm{DP}}|}, \tag{8}$$

where $|\,|$ denotes the area of the copied region or pasted region, $\cap$ denotes the intersection of two regions, $-$ denotes the difference between two regions, ψ_{C} denotes the pixels of the copied region, ψ_{P} denotes the pixels of the pasted region, $\tilde{\psi}_{\mathrm{DC}}$ denotes the pixels of detected copied region, and $\tilde{\psi}_{\mathrm{DP}}$ denotes the pixels of detected pasted region.

R_{DA} represents how well the algorithm performed in precisely locating the pixels of copy-move regions within the doctored image, while R_{FP} indicates the percentage of pixels that do not belong to duplicated regions but are detected as part of the duplicated regions by the proposed method. The closer R_{FP} is to 0 and R_{DA} is to 1, the higher the accuracy of the proposed scheme is.

4.3 Subjective Detection Effects of the Proposed Algorithm

To test the universal applicability of the proposed scheme, we conduct experiments using forged images in dataset [21]. The forged images, with size of 128×128, are in BMP format. Some of the detected results are shown in **Fig. 4**, in which the green region is the copied region and the blue region is the pasted region. Each row has three images, from left to right: the original image, forged image, and the detected result of the tampered image by the proposed algorithm. All the tampered images and the original images are available in [21].


(a)

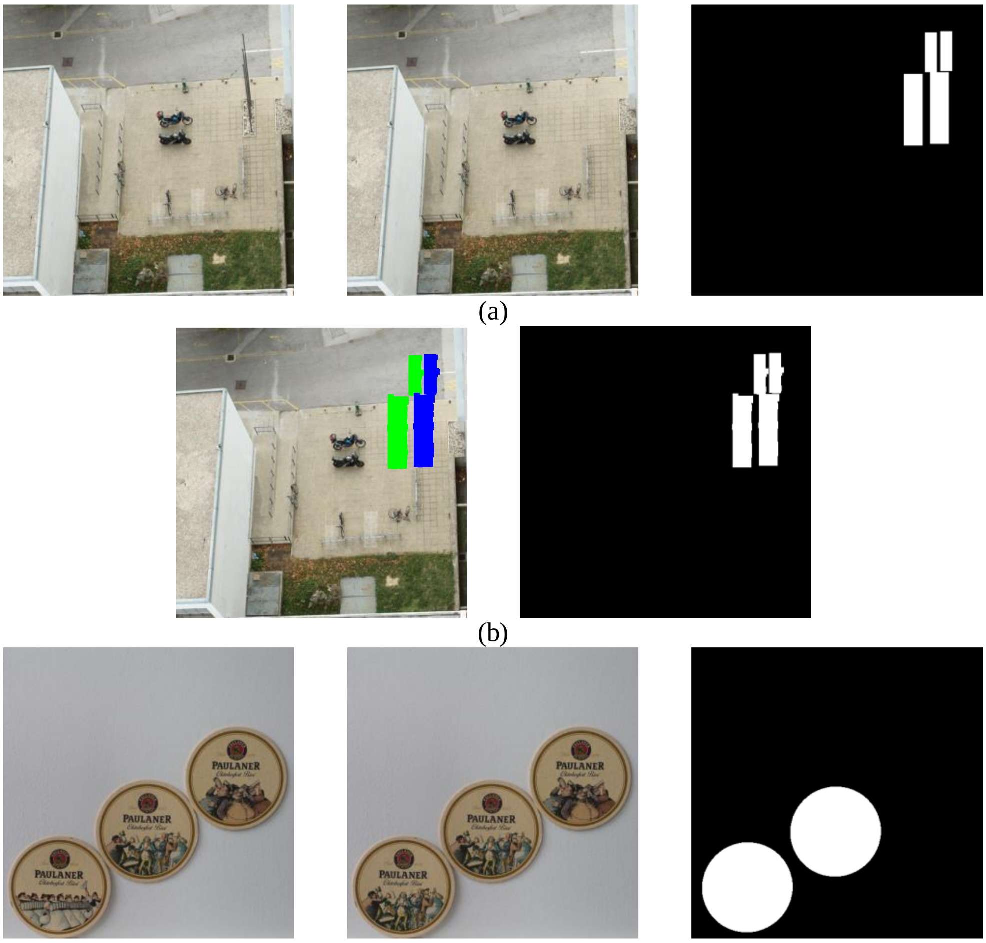
(b)

(c)

(d)

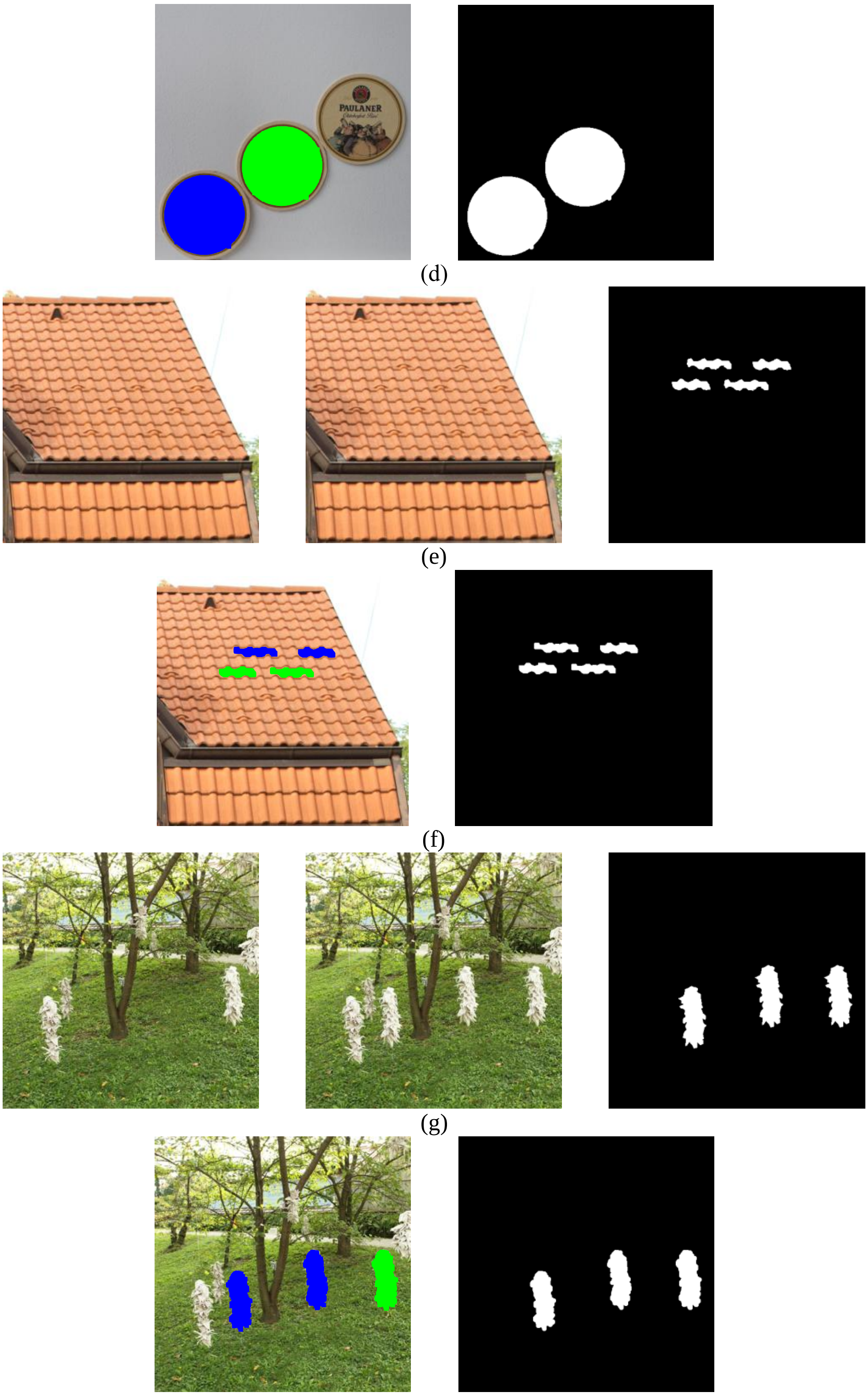
Fig. 4. Detected results of the proposed scheme: (a) AU_S_023, SP_S_023, detected SP_S_023; (b) AU_S_028, SP_S_028, detected SP_S_028; (c) AU_T_099, SP_T_099, detected SP_T_099; and (d) AU_T_109, SP_T_109, detected SP_T_109.

From **Fig. 4**, it is apparent that the proposed algorithm successfully detects the duplicated regions of the tampered images in the dataset [21]. The third column shows the marked copied (green) regions and pasted (blue) regions. However, in these examples, the tampered regions are only in the horizontal and vertical directions. Moreover, the masks of the copied region and pasted region are not given in [21]; therefore, it is difficult to evaluate the accuracy of the proposed scheme by analyzing the DAR (R_{DA}) and FPR (R_{FP}). In addition, the dataset [21] contains no color images. Fortunately, Tralic *et al*. provided an excellent work in [22], which makes up for the defects in [21]. The original color images, forged images, binary mask of forged images and various distorted images of both original and forged images are all available in the database [22] in which all images with size of 512×512 are in color. The images are in PNG format. We evaluate the proposed method using the color images in [22]. Some of the detected results are listed in **Fig. 5**. It is necessary to explain the naming convention: "001_O" denotes the original image, "001_F" denotes the forged image, and "001_B" denotes the binary mask of the forged image.


(a)

(b)

(c)



(d)

(e)

(f)

(g)

(h)

Fig. 5. Detected results of tampered images: (a) 002_O, 002_F, 002_B; (b) detected 002_F, mask of

detected results; (c) 006_O, 006_F, 006_B; (d) detected 006_F, mask of detected results; (e) 007_O, 007_F, 007_B; (f) detected 007_F, mask of detected results; (g) 027_O, 027_F, 027_B; and (h) detected 027_F, mask of detected results.

From **Fig. 5**, we can intuitively see that the proposed scheme can detect the copied and pasted regions of doctored color images for both irregular and circle shapes. The proposed scheme can detect multiple copy-move regions in **Fig. 5(a)**. It can also detect the circle-shaped region in **Fig. 5(c)** as well as irregular shapes in **Fig. 5(e)** and **Fig. 5(g)**. The visual output is also satisfactory. We also test the accuracy of the proposed algorithm with respect to R_{DA} and R_{FP} as discussed above. The results are listed in **Table 1**.

Table 1. R_{DA} and R_{FP} of the detected results from several tampered images

Criterion	**Fig. 5(b)**	**Fig. 5(d)**	**Fig. 5(f)**	**Fig. 5(h)**
R_{DA}	1.0000	1.0000	0.9662	0.9261
R_{FP}	0.0339	0.0033	0.0486	0.1164

As shown in **Table 1**, the R_{DA} values obtained by the proposed algorithm on the images in **Fig. 5(b)**, **(d)**, **(f)**, and **(h)** are close to or equal to 1, while their R_{FP} values on **Fig. 5(b)**, **(d)**, **(f)**, and **(h)** are close to 0. These results demonstrate that the proposed scheme is highly accurate at detecting the duplicated regions of the tampered images when the tampered regions are rectangles, circles or irregular regions at arbitrary locations within the same image.

From **Fig. 4**, **Fig. 5**, and **Table 1**, the precision of the proposed scheme is reflected in the intuitive visualization effect and the data at the pixel level. At the image level, we test 54 tampered images from the database folder “Sp-S”, 54 natural images from the “Au-S” folder, 126 doctored images from the “Sp-T” folder, and 126 natural images from the “Au-T” folder. The results obtained by testing these images [21] by the proposed method are listed in **Table 2**. N_{total} is the total number of image in each folder. The precision rate R_{P} and the recall rate R_{R} are calculated according to Eq. (5) and Eq. (6), respectively.

Table 2. Precision rate R_{P} and recall rate R_{R} of the tampered images in dataset [21]

Folder	N_{total}	N_{FF}	N_{IF}	N_{FI}	R_{P}	R_{R}
Sp-S	54	53		1	1	0.9814
Au-S	54		0			
Sp-T	126	126		0	1	1
Au-T	126		0			

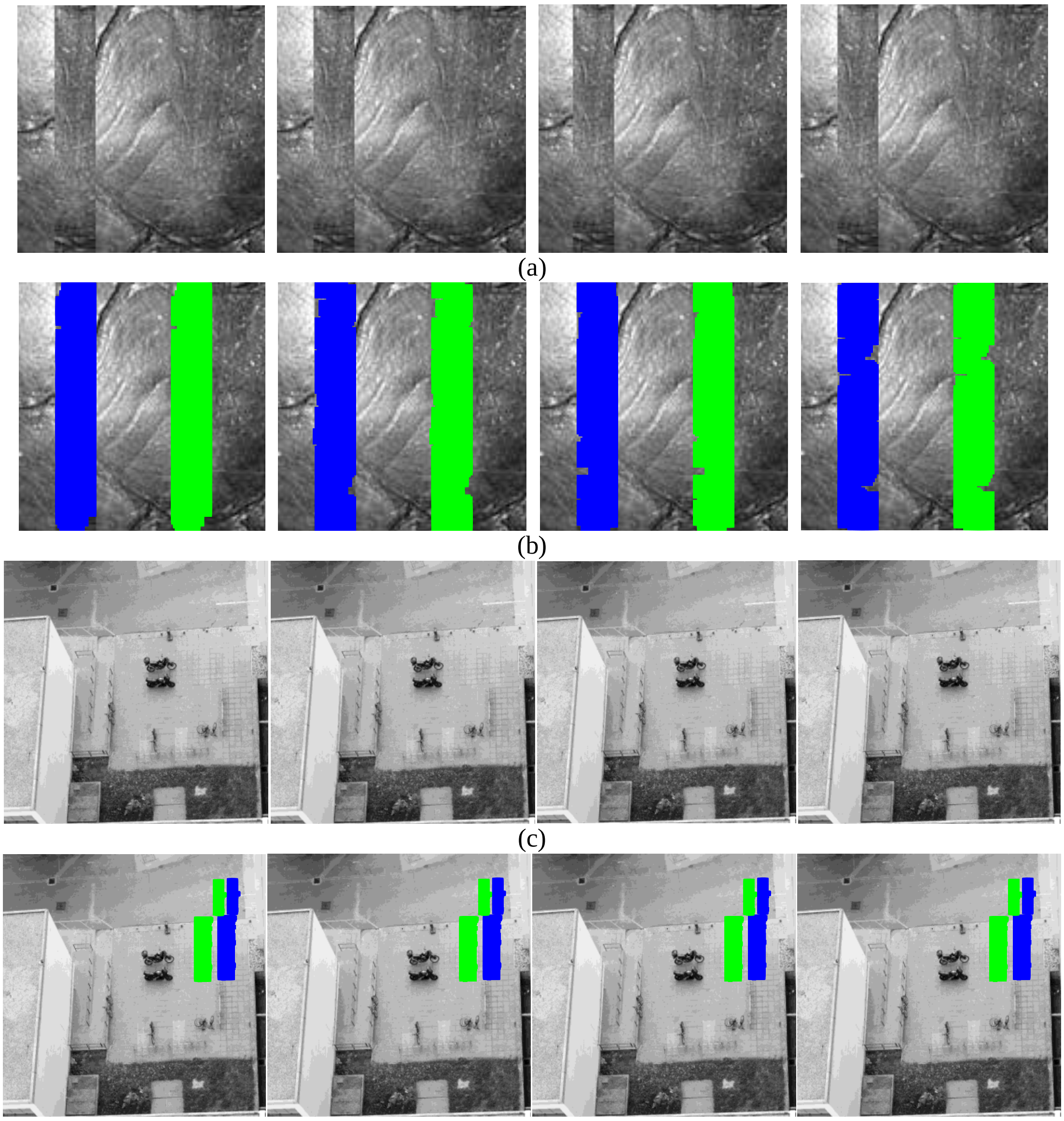
Regarding the results in **Table 2**, it is worth mentioning that the doctored images in the “Sp-S” folder were created by tampering the natural images in the “Au-S” folder, while the doctored images in the “Sp-T” folder were created by tampering the natural images in the “Au-T” folder. As shown in **Table 2**, R_{P} and R_{R} are almost always either close to or equal to 1, which indicates that the proposed algorithm has a relatively large application scope.

4.4 Robustness Test of the Proposed Algorithm

In an actual copy-move forgery, the attacker might conduct a series of post-processing operations after completing the basic copy-move forgery. Therefore, we conduct experiments to test the robustness of the proposed method against post-processing operations such as additive white Gaussian noise (AWGN), Gaussian blurring, and JPEG compression. The detected results are discussed below.

(1) AWGN

AWGN is one of the most typical types of noise in daily life. Therefore, to verify the proposed algorithm's anti-noise interference ability, AWGN is added to the images to be detected (shown in **Fig. 5**) at different signal-to-noise ratio (SNR): 40 dB, 30 dB, 20 dB, and 16 dB, respectively. The experimental results are manifested in **Fig. 6**. The values of R_{DA} and R_{FP} are listed in **Table 3**. Moreover, based on the results of numerous experimental tests, the detection effect will decline sharply when the SNR is less than 16 dB. For color images, the AWGN is added into each color channel; then, three channels of color images are converted into a grayscale image using the formula: $I = 0.299R + 0.587G + 0.114B$. Overall, the algorithm still reveals some ability to resist noise.



(a)

(b)

(c)

(d)

Fig. 6. Detected results of the tampered images with different AWGN: (a) SP_S_028 distorted by AWGN with SNR = 40 dB, SNR = 30 dB, SNR = 20 dB, and SNR = 16 dB; (b) detected results of the images in (a); (c) 002_F distorted by AWGN with SNR = 40 dB, SNR = 30 dB, SNR = 20 dB, and SNR = 16 dB; and (d) detected results of the images in (c).

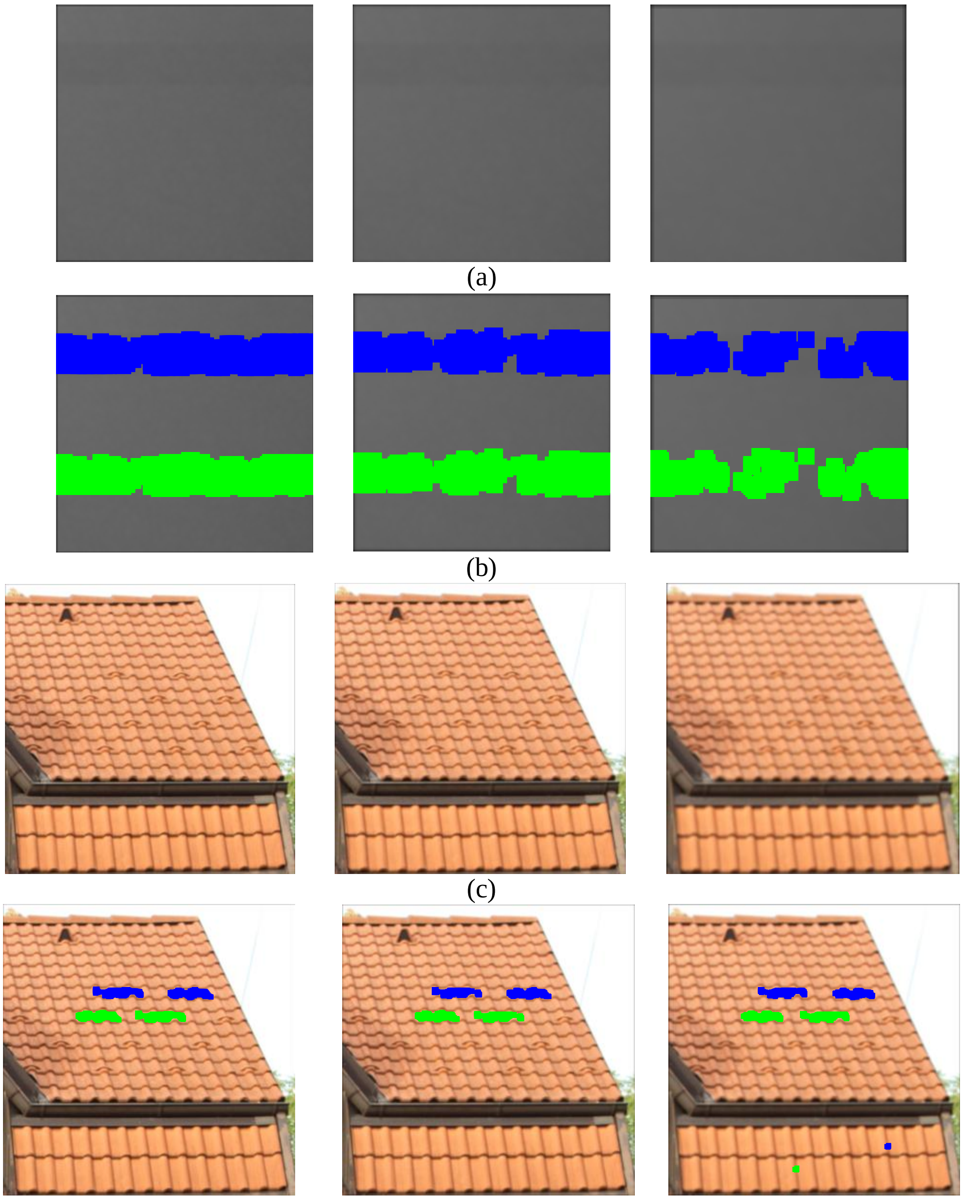
Table 3. R_{DA} and R_{FP} of the proposed method and other methods on images with AWGN

Image	**SNR**	**Criterion**	**Huang *et al.* [10]**	**Zhao and Guo [9]**	**Kang and Wei [8]**	**Fridrich *et al.* [6]**	**Proposed**
002_F	40	R_{DA}	1.0000	0.7391	0.8598	0.7428	1.0000
		R_{FP}	0.0116	0.4556	0.7298	0.7778	0.0087
	30	R_{DA}	1.0000	0.7391	0.3001	0.7428	1.0000
		R_{FP}	0.0116	0.4626	1.1935	0.7780	0.0087
	20	R_{DA}	0.9998	0.7391		0.7427	1.0000
		R_{FP}	0.0097	0.4421		0.7585	0.0087
	16	R_{DA}	1.0000	0.7391		0.7426	1.0000
		R_{FP}	0.0138	0.4384		0.7824	0.0081
006_F	40	R_{DA}	1.0000	0.9840	0.9931	1.0000	1.0000
		R_{FP}	0.0123	0.6679	0.2203	0.4291	0.0150
	30	R_{DA}	1.0000	0.9801	0.4158	1.0000	0.9999
		R_{FP}	0.0124	0.6795	1.2367	0.4318	0.0150
	20	R_{DA}	0.9998	0.9743		1.0000	0.9999
		R_{FP}	0.0126	0.6759		0.4276	0.0160
	16	R_{DA}	0.9995	0.9783		1.0000	0.9996
		R_{FP}	0.0127	0.6814		0.4295	0.0159

As shown in **Fig. 6**, the various copied and pasted regions are detected by the proposed method even in tampered images distorted by various levels AWGN. From **Table 3**, the R_{DA} and R_{FP} of the proposed method and the method in [10] are relatively satisfactory, indicating that both methods are robust to AWGN. Although the method in [9] detect a part of the copied and pasted regions, it also detect the left wall in 002_F and the gray region in 006_F as a part of tampered regions; the methods in [6] and [8] yield similar results. In addition, the method in [6] detects only the larger tampered region even after its related parameters are adjusted. The method in [8] fails to detect the tampered regions in the distorted tampered images with lower SNR values of AWGN. Overall, the results shown in **Fig. 6** and **Table 3** demonstrate that the proposed method is robust to AWGN to a certain extent.

(2) Gaussian blurring

Doctored images may be corrupted by Gaussian blurring to different degrees. In this experiment, we add Gaussian blurring using different parameters into forged grayscale and color images to test the robustness of the proposed scheme against Gaussian blurring. The image is filtered by Gaussian low-pass filter with size of $n_1 \times n_2$ and standard deviation σ. The doctored images are corrupted by Gaussian blurring with $n_1 = n_2 = 3$, $\sigma = 1$, $n_1 = n_2 = 5$, $\sigma = 1$, and $n_1 = n_2 = 5$, $\sigma = 2$, respectively. The results are shown in **Fig. 7** and the R_{DA} and R_{FP} values are listed in **Table 4**.


(a)

(b)

(c)

(d)

Fig. 7. Detected results of tampered images with varied Gaussian blurring: (a) SP_S_023 distorted by Gaussian blurring with $n_1 = n_2 = 3$, $\sigma = 1$, $n_1 = n_2 = 5$, $\sigma = 1$, and $n_1 = n_2 = 5$, $\sigma = 2$, respectively; (b) detected results of the images in (a); (c) 007_F distorted by Gaussian blurring with $n_1 = n_2 = 3$, $\sigma = 1$, $n_1 = n_2 = 5$, $\sigma = 1$, and $n_1 = n_2 = 5$, $\sigma = 2$, respectively; and (d) detected results of the images in (c).

Table 4. R_{DA} and R_{FP} of the proposed method and other methods on images with Gaussian blurring

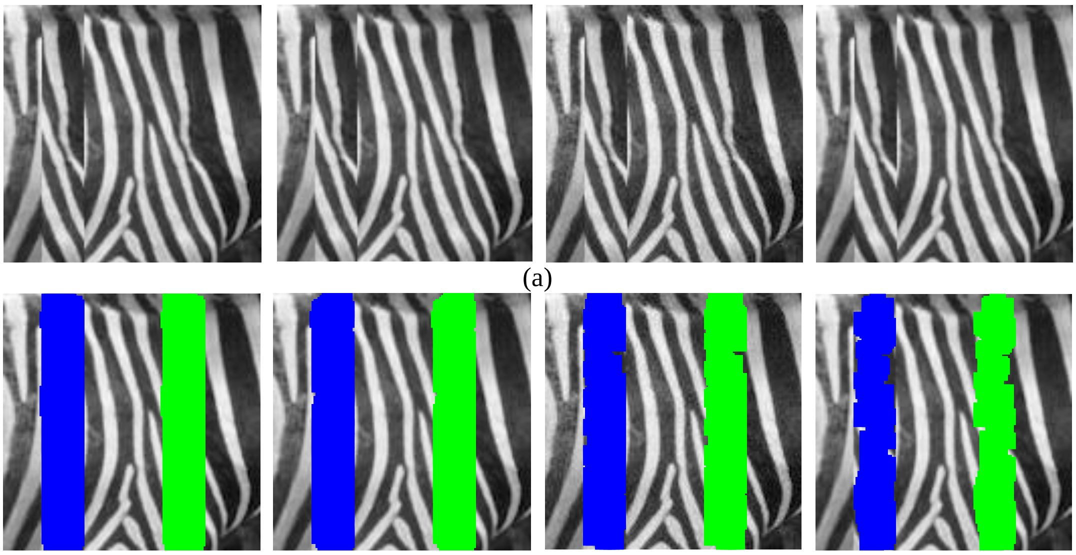
Image	**Gaussian Blurring**	**Criterion**	**Huang *et al.* [10]**	**Zhao and Guo [9]**	**Kang and Wei [8]**	**Fridrich *et al.* [6]**	**Proposed**
007_F	$n_1 = n_2 = 3$	R_{DA}	0.8714	0.9549			0.9100

		R_{FP}	0.6693	0.9389			0.1589
	$n_1 = n_2 = 5$ $\sigma = 1$	R_{DA}	0.8294	0.9384			0.8560
		R_{FP}	0.7931	0.9474			0.2027
	$n_1 = n_2 = 5$ $\sigma = 2$	R_{DA}	0.7914	0.9273			0.8428
		R_{FP}	0.9313	0.9510			0.2677
027_F	$n_1 = n_2 = 3$ $\sigma = 1$	R_{DA}	0.9065	0.9421	0.7008	0.9944	0.9492
		R_{FP}	0.1251	0.1576	0.4268	0.4873	0.1324
	$n_1 = n_2 = 5$ $\sigma = 1$	R_{DA}	0.8934	0.9416	0.6402	0.9931	0.9392
		R_{FP}	0.1378	0.1612	0.5819	0.4554	0.1174
	$n_1 = n_2 = 5$ $\sigma = 2$	R_{DA}	0.8753	0.9224	0.6256	0.9936	0.9205
		R_{FP}	0.1557	0.1357	0.5985	0.4608	0.1414

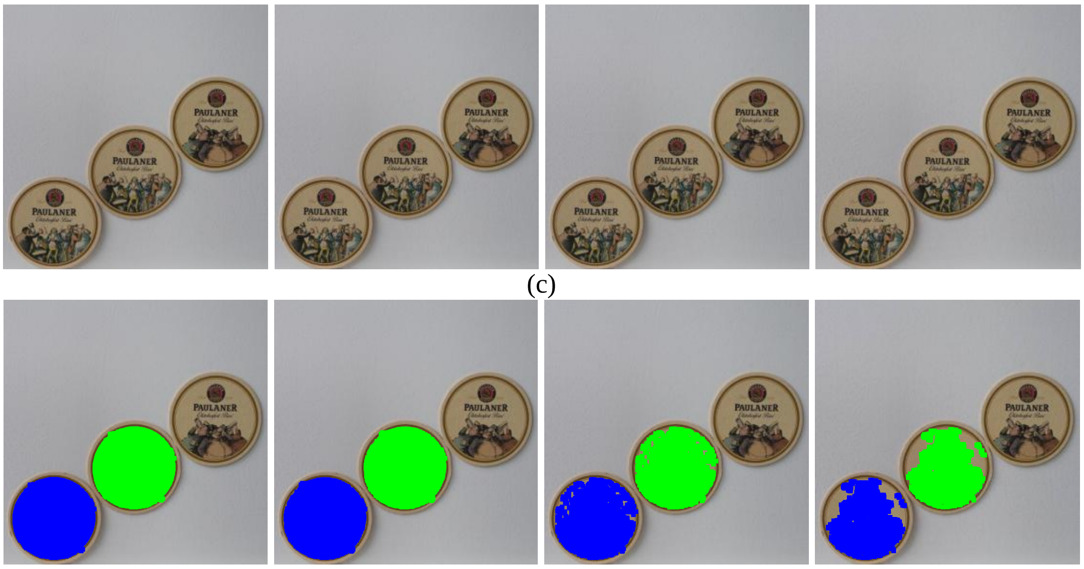
The images in **Fig. 7** indicate that the proposed scheme can detect duplicated regions in forged images corrupted by Gaussian blurring with different parameters. The results in **Table 4** show that the proposed scheme can detect both the copied and pasted regions and achieve higher accuracy than other methods including the method in [10]. These results indicate the advantages of introducing the c_{t}. Other methods, such as [6] and [8], incorrectly detected the sky or other roof tiles in 007_F as the duplicated regions. However, those are not the true tampered regions. The R_{FP} values exceed 1 represent that the methods not only detect the forged regions but also detect too many false regions.

(3) JPEG Compression

Images are usually stored in JPEG format. Therefore, it is necessary to test the algorithm's robustness against JPEG compression. In this experiment, the original image is resaved in JPEG format with different quality factors f_{Q}; the compressed JPEG images are used to test the effectiveness of proposed scheme. The JPEG quality factors ranges from 100 to 70. The detected results are shown in **Fig. 8** and the values of R_{DA} and R_{FP} are listed in **Table 5**.


(a)

(b)


(c)

(d)

Fig. 8. Detected results of JPEG compression with different f_Q: (a) SP_T_099 resaved as JPEG format with f_Q = 100, f_Q = 90, f_Q = 80, and f_Q = 70; (b) detected results of the images in (a); (c) 006_F resaved as JPEG format with f_Q = 100, f_Q = 90, f_Q = 80, and f_Q = 70; and (d) detected results of the images in (c).

Table 5. R_{DA} and R_{FP} of the proposed method and other methods on images with JPEG compression

Image	f_Q	Criterion	Huang *et al.* [10]	Zhao and Guo [9]	Kang and Wei [8]	Fridrich *et al.* [6]	Proposed
002_F	100	R_{DA}	0.9991	0.7386		0.7743	0.9993
		R_{FP}	0.0111	0.4694		0.7203	0.0314
	90	R_{DA}	0.9289	0.7377		0.7915	0.9909
		R_{FP}	0.0865	0.4723		0.7449	0.0343
	80	R_{DA}	0.3351	0.7273		0.7686	0.9150
		R_{FP}	1.9722	0.4978		0.7682	0.1124
	70	R_{DA}		0.6798		0.7429	0.3826
		R_{FP}		0.5996		0.7343	1.6140
006_F	100	R_{DA}	0.9986	0.9813		1.0000	0.9996
		R_{FP}	0.0151	0.6818		0.4404	0.0313
	90	R_{DA}	0.9566	0.9517		1.0000	0.9969
		R_{FP}	0.0545	0.7061		0.4450	0.0354
	80	R_{DA}	0.7680	0.9341		1.0000	0.9819
		R_{FP}	0.3087	0.7176		0.4286	0.0496
	70	R_{DA}	0.6480	0.9093		1.0000	0.8458
		R_{FP}	0.5445	0.7341		0.4395	0.1949

From **Fig. 8**, the proposed scheme is robust to JPEG compression on both grayscale and color images. The results in **Table 5** indicate that the method in [8] fails to detect the tampered images processed by JPEG compression. In contrast, the proposed scheme detect the duplicated regions in tampered images in JPEG format whose f_{Q} ranges from 100 to 70, improving the method in [10]. The methods in [6] and [9] are relatively stable, but **Table 5** shows that [6, 9, 10] still falsely detect the wall in 002_F and gray region or the rightmost badge in 006_F as tampered regions, which do not occur using the proposed scheme.

As shown in **Fig. 6**, **Fig. 7**, and **Fig. 8**, the proposed scheme is robust to AWGN, Gaussian blurring, and JPEG compression within acceptable limits. The results in **Table 3**, **Table 4**, and **Table 5** also reveal the effectiveness of the proposed method, which achieves better results than the method in [10]. The methods in [6] and [9] are relatively stable against the post-processing methods mentioned above, but they incorrectly detect regions such as tiles, walls, ground, and gray background as tampered regions. The scheme in [8] is susceptible to various post-processing methods such as JPEG compression and Gaussian blurring. The proposed method is comparatively more accurate than the other tested methods.

4.5 Comparison with Other Algorithms

In this section, we compare our algorithm with the algorithms in [6, 8-10] from feature and time complexity perspectives. In all the experiments, color images are converted into grayscale images. The time complexity experiment follows these steps: dividing the image into overlapping image blocks, extracting feature vectors, searching for similar feature vectors, counting the number of feature vectors, finding the main transfer vectors, and visual output. Both grayscale images (128×128) and color images (512×512) are used in these experiments; all the images are available in databases [21] and [22]. The feature and time complexity comparisons are listed in **Table 6** and **Table 7**, respectively. The notation N_{a} in **Table 6** means that a feature vector needs to be compared with N_{a} adjacent feature vectors to find similar feature vectors. The unit of time in **Table 7** is seconds (s).

Table 6. Feature comparison of different algorithms

Item	**Huang *et al.* [10]**	**Zhao and Guo [9]**	**Kang and Wei [8]**	**Fridrich *et al.* [6]**	**Proposed**
Block size *b*	8	8	20	16	8
Feature	Quantized DCT coefficients	Singular values of DCT coefficients	Singular values	Quantized DCT coefficients	Quantized DCT coefficients
Feature dimensions	16	16	20	256	16
N_{a}	3	1	1	1	3

Table 7. Time complexity comparison of different algorithms

Image / Average Time	**Huang *et al.* [10]**	**Zhao and Guo [9]**	**Kang and Wei [8]**	**Fridrich *et al.* [6]**	**Proposed**
SP_S_023	6.35		4.56		22.11
SP_S_028	3.11	12.68	4.59	3.75	4.68
SP_T_099	3.26	20.60	4.33	9.67	12.95
SP_T_109	3.12	19.49	4.39	9.18	4.61

Average time (s)	3.96	17.60	4.47	7.54	11.09
002_F	60.11	4,019.98	78.02	1,341.41	1,592.06
006_F	87.09	895.21	84.44	245.48	2,933.06
007_F	105.84	4,698.07			2,042.86
027_F	53.45	9,050.05	84.94	5,547.30	1,855.09
Average time (s)	76.62	4,665.83	82.46	2,378.07	2,105.77

As shown in **Table 7**, the proposed scheme has a slightly higher time complexity than the other block-based copy-move detection methods. This aspect is one of the directions for improvement in future work. The methods in [6] and [9] fail to detect the duplicated regions in SP_S_023 that consist of gray sky. The schemes in [6] and [8] fail to detect the copied and pasted regions in 007_F where the tiles are the duplicated regions. The proposed scheme detects the duplicated regions in all the experimental images.

5. Conclusions

An improved copy-move image forgery detection scheme is proposed in this paper. After testing the tampered images in the Columbia image-splicing detection evaluation dataset and the CoMoFoD database, the proposed method detects most of the copy-move tampered images, demonstrating its wide practicability. Moreover, based on the results of the robustness test experiments, the proposed scheme is robust to AWGN, Gaussian blurring, and JPEG compression to a reasonable extent. Compared with the other tested algorithms, the proposed method achieved higher accuracy. However, it also results in a high computational burden, which is a direction for future improvement. The proposed scheme also needs to be improved to detect copied and pasted regions affected by operations such as rotation and scaling.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61702303, No. 61201371), the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022), and the Natural Science Foundation of Shandong Province, China (No. ZR2017MF020, No. ZR2015PF004). Zhi Zhang, Dongyan Wang, and Chengyou Wang conceived the algorithm; Zhi Zhang and Dongyan Wang designed and performed the experiments; Chengyou Wang and Xiao Zhou analyzed the results; Dongyan Wang drafted the manuscript; Zhi Zhang and Dongyan Wang revised the manuscript; Chengyou Wang and Xiao Zhou supervised the research project.

References

[1] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digital Investigation*, vol. 10, no. 3, pp. 226-245, Oct. 2013. Article (CrossRef Link).

[2] Photo Tampering throughout History, the pictures of Senator John Kerry and Jane Fonda. Article (CrossRef Link).

[3] Photo Tampering throughout History, the actual and doctored images of Iranian missile test. Article (CrossRef Link).

[4] W. C. Hu, W. H. Chen, D. Y. Huang, and C. Y. Yang, "Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3495-3516, Mar. 2016. Article (CrossRef Link).

[5] Y. Dai and S. H. Su, "A diploma anti-forgery system based on lightweight digital signatures," in *Proc. of the 10th Inernational Conference on Computational Intelligence and Security*, Kunming, China, Nov. 15-16, pp. 647-651, 2014. Article (CrossRef Link).

[6] J. Fridrich, D. Soukalm, and J. Lukáš, "Detection of copy-move forgery in digital images," in *Proc. of the Digital Forensic Research Workshop*, Cleveland, OH, USA, 10 pages, Aug. 5-8, 2003. Article (CrossRef Link).

[7] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Technical Report*, TR 2004-515, Deparment of Computer Science, Dartmouth College, 2004. Article (CrossRef Link).

[8] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proc. of the International Conference on Computer Science and Software Engineering*, Wuhan, China, Dec. 12-14, 2008, pp. 926-930. Article (CrossRef Link).

[9] J. Zhao and J. C. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Science International*, vol. 233, no. 1-3, pp. 158-166, Dec. 2013. Article (CrossRef Link).

[10] Y. P. Huang, W. Lu, W. Sun, and D. Y. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic Science International*, vol. 206, no. 1-3, pp. 178-184, Mar. 2011. Article (CrossRef Link).

[11] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Taipei, Taiwan, pp. 1053-1056, Apr. 19-24, 2009. Article (CrossRef Link).

[12] I. Amerini, M. Barni, R. Caldelli, and A. Costanzo, "Removal and injection of keypoints for SIFT-based copy-move counter-forensics," *EURASIP Journal on Information Security*, vol. 2013, article number: 8, 12 pages, Dec. 2013. Article (CrossRef Link).

[13] B. Xu, J. W. Wang, G. J. Liu, and Y. W. Dai, "Image copy-move forgery detection based on SURF", in *Proc. of the 2nd International Conference on Multimedia Information Networking and Security*, Nanjing, China, pp. 889-892, Nov. 4-6, 2010. Article (CrossRef Link).

[14] R. C. Pandey, R. Agrawal, S. K. Singh, and K. K. Shukla, "Passive copy move forgery detection using SURF, HOG and SIFT features," in *Proc. of the 3rd International Conference on Frontiers in Intelligent Computing: Theory and Applications*, Reykjavík, Iceland, pp. 659-666, Nov. 14-15, 2014. Article (CrossRef Link).

[15] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," *Forensic Science International*, vol. 171, no. 2-3, pp. 180-189, Sept. 2007. Article (CrossRef Link).

[16] A. V. Malviya and S. A. Ladhake, "Pixel based image forensic technique for copy-move forgery detection using auto color correlogram," in *Proc. of the 7th International Conference on Communication, Computing and Virtualization*, Mumbai, India, pp. 383-390, Feb. 26-27, 2016. Article (CrossRef Link).

[17] F. Yang, J. W. Li, W. Lu, and J. Weng, "Copy-move forgery detection based on hybrid features," *Engineering Applications of Artificial Intelligence*, vol. 59, pp. 73-83, Mar. 2017. Article (CrossRef Link).

[18] D. Vaishnavi and T. S. Subashini, "A passive technique for image forgery detection using contrast context histogram features," *International Journal of Electronic Security and Digital Forensics*, vol. 7, no. 3, pp. 278-289, Jul. 2015. Article (CrossRef Link).

[19] W. Q. Luo, J. W. Huang, and G. P. Qiu, "Robust detection of region-duplication forgery in digital image," in *Proc. of the 18th International Conference on Pattern Recognition*, Hong Kong, China, vol. 4, pp. 746-749, Aug. 20-24, 2006. Article (CrossRef Link).

[20] Q. M. Fu, X. Zhou, C. Y. Wang, and B. C. Jiang, "Mathematical relation between APBT-based and DCT-based JPEG image compression schemes," *Journal of Communications*, vol. 11, no. 1, pp. 84-92, Jan. 2016. Article (CrossRef Link).

[21] T. T. Ng and S. F. Chang, "A data set of authentic and spliced image blocks," *ADVENT Technical Report*, 203-2004-3, Columbia University, Jun. 2004. Article (CrossRef Link).

[22] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD - New database for copy-move forgery detection," in *Proc. of the 55th International Symposium ELMAR*, Zadar, Croatia, pp. 49-54, Sept. 25-27, 2013. Article (CrossRef Link).

[23] 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, no. 6, pp. 1841-1854, Dec. 2012. Article (CrossRef Link).

Zhi Zhang was born in Shandong province, China, in 1992. He received his B.E. degree in electronic information engineering from Shandong University of Science and Technology, China, in 2016. He is currently pursuing his M.E. degree in information and communication engineering at Shandong University, China. His current research interests include digital image processing and computer vision.

Dongyan Wang was born in Shandong province, China, in 1996. She is currently pursuing her B.E. degree in computer science and technology at Shandong University, Weihai, China. Her current research interests include digital image processing and computer vision.

Chengyou Wang was born in Shandong province, China, in 1979. He received his B.E. degree in electronic information science and technology from Yantai University, China, in 2004, and his M.E. and Ph.D. degrees in signal and information processing from Tianjin University, China, in 2007 and 2010, respectively. He is currently an associate professor and supervisor of postgraduate students at Shandong University, Weihai, China. His current research interests include digital image/video processing and analysis, computer vision, pattern recognition, and machine learning.

Xiao Zhou was born in Shandong province, China, in 1982. She received her B.E. degree in automation from Nanjing University of Posts and Telecommunications, China, in 2003; her M.E. degree in information and communication engineering from Inha University, Korea, in 2005; and her Ph.D. degree in information and communication engineering from Tsinghua University, China, in 2013. She is currently a lecturer and supervisor of postgraduate students at Shandong University, Weihai, China. Her current research interests include wireless communication technology, image communication, and computer vision.