Hindawi
Security and Communication Networks
Volume 2018, Article ID 6853696, 11 pages
https://doi.org/10.1155/2018/6853696

Research Article

Perceptual Hashing-Based Image Copy-Move Forgery Detection

Huan Wang and Hongxia Wang

School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China

Correspondence should be addressed to Hongxia Wang; hxwang@swjtu.edu.cn

Received 29 September 2017; Revised 10 December 2017; Accepted 20 December 2017; Published 22 January 2018

Academic Editor: Zhenxing Qian

This paper proposes a blind authentication scheme to identify duplicated regions for copy-move forgery based on perceptual hashing and package clustering algorithms. For all fixed-size image blocks in suspicious images, discrete cosine transform (DCT) is used to obtain their DCT coefficient matrixes. Their perceptual hash matrixes and perceptual hash feature vectors are orderly addressed. Moreover, a package clustering algorithm is proposed to replace traditional lexicographic order algorithms for improving the detection precision. Similar blocks can be identified by matching the perceptual hash feature vectors in each package and its adjacent package. The experimental results show that the proposed scheme can locate irregular tampered regions and multiple duplicated regions in suspicious images although they are distorted by some hybrid trace hiding operations, such as adding white Gaussian noise and Gaussian blurring, adjusting contrast ratio, luminance, and hue, and their hybrid operations.

1. Introduction

Copy-move forgery as a popular digital image tampering technology is extensively used by forgers. In a digital image, some regions are copied and then pasted into other regions in this same image to achieve the purpose of hiding some targets or emphasizing some important objects [1]. Its authenticity is broken. Since the original regions and the duplicated regions come from the same image, their most important characteristics, such as the color palettes, noises, and dynamic ranges, are compatible with the remainder of the image [2]. One may neglect this malicious operation if forgers deliberately hide the tampering traces. A typical copy-move forgery example is shown in Figure 1, where the traffic flow is exaggerated by tampering cars. It is urgent to propose effective copy-move forgery detection methods to detect and locate the tampered regions for digital images. Blind authentication for copy-move forgery mainly focuses on the identifying of tampered regions in digital images without any additional information except for themselves. Based on this advantage, it becomes to a valuable research in image authentication fields [3].

Block-based methods and keypoint-based methods are the common techniques for copy-move forgery detection. Block-based methods indicate that a suspicious image is divided into overlapped and fix-sized blocks. The tampered regions can be identified by matching the similar feature vectors that are extracted from the blocks. Fridrich et al. in [1] first proposed a block-based detection scheme using quantized discrete cosine transform (DCT) coefficients, which is one of the landmark methods for copy-move forgery detection. Popscu and Farid in [4] presented a novel method that use principal component analysis (PCA) to derive an alternative representation for each image block. However, it cannot resist other robustness attacks and identify some little tampered regions. Babak and Stanislav in [5] presented a copy-move forgery detection scheme to extract image features for overlapped blocks based on blur moment invariants. Cao et al. in [6] exploited the mean of DCT coefficients to propose their algorithm that not only can resist the attacks of blurring and additive noise operations, but also considers the detection accuracy rate (DAR) and false positive rate (FPR). However, it is weak to resist the attack of hue or contrast ratio adjustments. Thajeel and Sulong in [7] presented an approach to improve the detection precision based on completed robust local binary pattern. Wang et al. in [8] proposed a copy-move forgery detection scheme to improve the detection precision based on DCT and package clustering algorithms. However,

(a) (b)

Figure 1: An example of copy-move forgery: (a) an original image and (b) a copy-move forgery image.

the robustness of feature vectors has been concentrated less. Zhong et al. in [9] presented a scheme that divides the tampered image into overlapped circular blocks. The features of circular blocks are extracted by the discrete radial harmonic Fourier moments. This method obtains outstanding performance under image geometrical distortions. Dixit et al. in [10] proposed a method for detecting copy-move forgery using stationary wavelet transform. The detection accuracy of the proposed method is also considered. Bi and Pun in [11] presented a fast reflective offset guided searching method for image copy-move forgery detection. It aims to reduce the computational complexity. The block-based methods mentioned above need to divide the image into overlapped and fix-sized blocks and then handle each of them. These algorithms can resist some plain postprocessing operations, such as JPEG compression, blurring, and noise interference. However, they did not achieve satisfactory results to resolve a common problem of reducing similar region matching times.

Keypoint-based methods rely on the identification of high-entropy image regions [12]. A feature vector can be extracted for each keypoint. Fewer feature vectors are estimated since the number of keypoints is reduced. Therefore, keypoint-based methods theoretically have lower computational costs for feature vectors matching and postprocessing. Amerini et al. in [12, 13] presented scale invariant feature transform (SIFT) to filter, sort, and classify the keypoint pairs for copy-move forgery detection. Li et al. in [14] try to reduce the similar region matching times and improve the DAR and FPR by segmenting a suspicious image into nonoverlapped patches. Wang et al. in [15] introduced a keypoints-based image passive detecting method based on Harris detector and region growth technology. It is robust for JPEG compression, gamma adjustment, and luminance enhancement. Li et al. in [16] proposed a hierarchical cluster algorithm based on maximally stable color region detector and Zernike moments to extract all keypoint features. Wang et al. in [17] presented a method to segment a suspicious image into irregular superpixels that are classified into smooth, texture, and strong texture. The stable image keypoints can be extracted from each superpixel. The above-mentioned algorithms have moved the copy-move forgery detection field ahead rapidly. However, they did not achieve satisfactory results on the improving of DAR and FPR in order to reduce the matching times. The resistance for other postprocessing operations is less considered, such as adjusting contrast ratio, luminance, hue, and their hybrid operations.

Perceptual hashing [18] is a class of one-way mappings from multimedia presentations to perceptual hash values in terms of the perceptual content. It is widely applied to perform multimedia content identification, retrieval, and authentication. In similar image searching and target tracking, perceptual hash algorithms are applied to generate fingerprints for digital images and then are used to compare them with each other. In addition, perceptual hash values are robust to take into account transformations or "attacks" on a given input and, yet, flexible enough to distinguish between dissimilar files. Such attacks include skew, contrast adjustment and different compression. Perceptual hash values are analogous if features are similar [19]. In a copy-move forgery image, the copy regions are similar with their paste regions. Therefore, perceptual hash algorithms can also be used to generate robust features for detecting the tampered regions.

In this study, a passive authentication scheme is proposed to perform authenticating for copy-move forgery based on perceptual hashing. The novelty of the proposed scheme includes the following: (1) Using perceptual hashing algorithms, the feature vectors of image blocks are robust for improving the DAR and FPR. (2) A package clustering algorithm is used to replace traditional lexicographic order methods to reduce the block matching times, where each package is used to represent a cluster. (3) Using perceptual hash algorithms, the proposed method can effectively identify and locate multiple duplicated regions in digital images that may be distorted by adding white Gaussian noise and Gaussian blurring, adjusting contrast ratio, luminance, hue, and their hybrid operations.

The rest of this paper is organized as follows. Section 2 introduces the proposed method. Section 3 shows the performance of the proposed scheme with a series of experiments. Finally, this paper is concluded in Section 4.

2. The Proposed Scheme

It is impossible in general that there are two identical regions in a naturally formed picture unless it contains large area

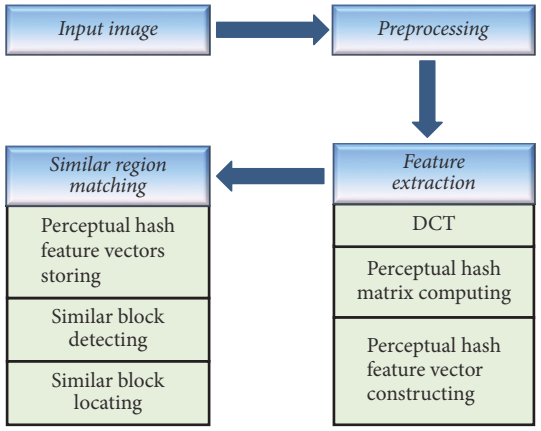

Figure 2: The framework of the proposed copy-move forgery scheme.

smooth regions, such as a blackboard or a piece of blue sky [20]. In this study, we suppose that all images do not contain large area smooth regions.

It is an incontestable fact that each suspicious image contains at least two similar regions, that is, an original region and a copy-move forgery region, if the suspicious image is tampered with copy-move forgery. By concluding many existing schemes, the task of passive authentication for copy-move forgery is to detect and locate tampered regions for suspicious images. In our proposed method, two main steps, that is, feature extraction and feature matching, are separately introduced. In the feature extraction step, perceptual hashing algorithms are extended to generate perceptual hash feature vectors that can be used to represent the image blocks in a suspicious image. In feature matching step, the idea of a package clustering algorithm is used to replace general lexicographically sorting algorithms to improve the detection precision and reduce the feature vector comparing times. Figure 2 shows the framework of the proposed scheme.

2.1. Preprocessing Operation. Let A be a suspicious image. It should be converted into a gray-scale image by $I = 0.299\mathrm{R} + 0.587\mathrm{G} + 0.114\mathrm{B}$ if it is a color image, where R, G, and B represent the red, green, and blue components of A, respectively, and I represents the pixel value of gray-scale image.

2.2. Feature Extraction Using Perceptual Hashing. In this step, suspicious image A is divided into different image blocks. DCT is applied to generate the DCT coefficient matrix for each image block. Finally, perceptual hashing is used to extract a perceptual hash feature vector for each image block according to its generated DCT coefficient matrix. The details of the feature extracting algorithm are shown in Algorithm 1.

In Step 1, suspicious image A with the size of $H \times W$ pixels is divided into $(H-b+1) \times (W-b+1)$ overlapping blocks by sliding a square window with the size of $b \times b$ pixels along with image A from the upper-left corner right down to the lower-right corner; that is, the adjacent overlapping blocks only have

Input: A suspicious gray-scale image A.
Output: All perceptual hash feature vectors for image blocks in A.

Step 1. Suspicious image A is divided into $(W-b+1) \times (H-b+1)$ overlapping blocks, denoted as B_{ij}, where $0 < b \ll W$, $0 < b \ll H$, $1 \le i \le (W-b+1)$, and $1 \le j \le (H-b+1)$.
Step 2. For each block B_{ij}
Step 3. The pixel mean of B_{ij}, denoted as P_{ij}, is computed.
Step 4. DCT is applied to generate the coefficient matrix for block B_{ij}, denoted as C_{ij}.
Step 5. The coefficient matrix C_{ij} is divided into four sub-blocks, denoted as C_{ij}^1, C_{ij}^2, C_{ij}^3, and C_{ij}^4, respectively.
Step 6. The mean of the first sub-block C_{ij}^1 is calculated, denoted as m_{ij}.
Step 7. The perceptual hashing matrix for each sub-block C_{ij}^k is computed, denoted as H_{ij}^k, where $k \in \{1, 2, 3, 4\}$.
Step 8. Each perceptual hashing matrix H_{ij}^k is converted into a decimal number, denoted as d_{ij}^k, to represent feature value for block B_{ij}, where $k \in \{1, 2, 3, 4\}$.
Step 9. The feature vector of block B_{ij} is created, denoted as $F_{ij} = (P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4)$, according to its pixel mean and four feature values.
Step 10. End For

Algorithm 1: Feature extraction.

one different row or column. Each block is denoted as B_{ij}, where $1 \le i \le (H-b+1)$, $1 \le j \le (W-b+1)$, i and j indicate the starting point of the block's row and column, respectively. Therefore, the original regions and their copy-move forgery regions are also divided into different blocks in which there is at least a pair of identical or similar blocks. The main task of the proposed scheme is to detect and locate these identical or similar blocks in pairs.

In Steps 2–10, the feature vector of each block is computed using DCT and perceptual hashing algorithms. It is unideal to directly use pixel values to match similar blocks in suspicious images since the forgers may distort the content of the tampered images. An ideal method is extracting robust features to represent blocks and then the similar blocks can be diagnosed by matching these robust features. The purpose is to strengthen the robustness and improve the detection accuracy of the proposed scheme. In this algorithm, perceptual hash features play this role, which are used to represent image blocks.

In Step 3, the pixel mean of image block B_{ij}, denoted as P_{ij}, is calculated as follows:

$$P_{ij} = \frac{\sum_{x=1}^{b} \sum_{y=1}^{b} f_{ij}(x, y)}{b^2}, \quad (1)$$

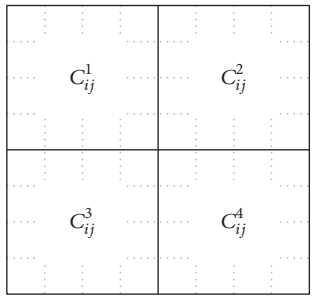

Figure 3: The method of dividing a block into four subblocks.

where $f_{ij}(x, y)$ represents the pixel value of xth row and yth column in B_{ij}. For the pair of two identical or similar image blocks, their pixel means are also identical or similar.

In Step 4, DCT is applied to exploit the DCT coefficient matrix for each block B_{ij}, denoted as C_{ij}, where the DCT coefficient matrix has the same size with block B_{ij}, $1 \le i \le (H - b + 1)$, and $1 \le j \le (W - b + 1)$.

In Step 5, coefficient matrix C_{ij} is divided into four subblocks. A typical characteristic of DCT is that the energy of an image focuses on the low frequency part and the high frequency coefficients play insignificant roles. This means that not all elements are equally important in C_{ij} and the top-left part of C_{ij} represents most features of block B_{ij}. In the proposed method, each DCT coefficient matrix C_{ij} will be equally divided into four subblocks, denoted as C_{ij}^1, C_{ij}^2, C_{ij}^3, and C_{ij}^4, as shown in Figure 3.

In Steps 6–9, the feature vector of block B_{ij} is created using perceptual hashing algorithm. According to the typical characteristic of DCT, the energy of the first subblock can be used to approximately represent the energy of whole block B_{ij}. This means that the average energy of block B_{ij} can be approximately represented by the energy of first subblock C_{ij}^1. In Step 6, the average energy of subblock C_{ij}^1, denoted as m_{ij}^1, is calculated as follows:

$$m_{ij}^1 = \frac{\sum_{x=1}^{b/2} \sum_{y=1}^{b/2} c_{ij}^1(x, y)}{(b/2)^2}, \tag{2}$$

where $c_{ij}^1(x, y)$ indicates the element of xth row and yth column in subblock C_{ij}^1.

In Step 7, the perceptual hash matrixes of the four subblocks C_{ij}^1, C_{ij}^2, C_{ij}^3, and C_{ij}^4, denoted as H_{ij}^1, H_{ij}^2, H_{ij}^3, and H_{ij}^4, respectively, are generated according to the average energy of subblock C_{ij}^1,that is, m_{ij}^1. Therefore, $\forall h_{ij}^k(x, y) \in H_{ij}^k$ is calculated as follows:

$$h_{ij}^k(x, y) = \begin{cases} 1, & c_{ij}^k(x, y) \in C_{ij}^k,\ c_{ij}^k(x, y) \ge m_{ij}^1 \\ 0, & c_{ij}^k(x, y) \in C_{ij}^k,\ c_{ij}^k(x, y) < m_{ij}^1, \end{cases} \tag{3}$$

where $1 \le x \le b/2$, $1 \le y \le b/2$, and $k \in \{1, 2, 3, 4\}$. Obviously, perceptual hash matrix H_{ij}^k can be considered as a perceptual digest from an image block to a binary matrix. It is used to represent the image block.

In Step 8, perceptual hash matrixes are converted into decimal numbers. In practical application, it is easier to calculate and store decimal numbers than binary matrixes. The four perceptual hash matrixes H_{ij}^1, H_{ij}^2, H_{ij}^3, and H_{ij}^4 are converted into four decimal numbers, denoted as d_{ij}^1, d_{ij}^2, d_{ij}^3, and d_{ij}^4, respectively, along with their rows.

In Step 9, the perceptual hash feature vector of block B_{ij} is created. For block B_{ij}, it has five special values that are considered as above, that is, the pixel mean P_{ij} and the four decimal numbers d_{ij}^1, d_{ij}^2, d_{ij}^3, and d_{ij}^4. In order to more accurately represent block B_{ij}, its perceptual hash feature vector, denoted as F_{ij}, is constructed as follows:

$$F_{ij} = \left(P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4\right). \tag{4}$$

Obviously, perceptual hash feature vector F_{ij} has the properties of simpleness and robustness. Therefore, it can be considered as the feature vector for image block B_{ij}.

2.3. Similar Region Matching. In the matching stage of the existing methods, their feature vectors are sorted first by some sorting algorithms, such as traditional lexicographic order algorithms, and then used to detect and locate the similar blocks using block matching methods. However, two kinds of issues in these existing methods should be improved to achieve better matching results. One is the block matching times, it will cause that the proposed matching algorithm has higher time complexity. Another is the precision of locating duplicated regions, which is dissatisfactory. In our proposed scheme, a package clustering algorithm is proposed to detect and locate the tampered regions with the purpose of improving the detection precision. The details of the proposed similar region matching algorithm are described in Algorithm 2.

In Algorithm 2, Steps 1 and 2 construct a package clustering algorithm that stores all perceptual hash feature vectors into the prepared packages according to the pixel means of blocks. Steps 4–7 compare all perceptual hash feature vectors to detect and locate the similar blocks according to the proposed package matching rule.

In Step 1, a set of packages is created. Let n be a preset threshold that represents the maximum capacity of all packages. Therefore, $\xi = (\lfloor 256/n \rfloor + 1)$ packages are created, denoted as $PA_1, PA_2, \ldots$, and PA_ξ, since the suspicious image is a gray-scale image (its pixel range is zero to 255), where $\lfloor\ \rfloor$ is a floor function.

In Step 2, all perceptual hash feature vectors are stored into the ξ packages. Let B_{ij} be a block and $F_{ij} = (P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4)$ be the perceptual hash feature vector of block B_{ij}. Then, block B_{ij} will be put into package PA_θ, where $\theta = (\lfloor P_{ij}/n \rfloor + 1)$. For example, assume $i = 6$, $j = 5$, $n = 4$, and $P_{65} = 129$. Block B_{65} will be put into package PA_{33}, where $(\lfloor P_{65}/n \rfloor + 1) = (\lfloor 129/4 \rfloor + 1) = 33$. This indicates that the pixel mean range of package PA_{33} is $\{128, 129, 130, 131\}$.

For any two image blocks B_{ij} and B_{mn}, their pixel values are similar if the two image blocks are duplicated. Naturally, their average pixel values P_{ij} and P_{mn} are also similar, where

Input: All perceptual hash feature vectors $F_{ij} = (P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4)$, where $1 \le i \le (H - b + 1)$ and $1 \le j \le (W - b + 1)$, which are the output of Algorithm 1.

Output: A map that includes the detection results.

Step 1. Creating ξ packages, denoted as PA_1, $PA_2, \ldots$, and PA_ξ, where $\xi = \lfloor 256/n \rfloor + 1$ and n is a preset threshold.

Step 2. All perceptual hash feature vectors $F_{ij} = (P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4)$ are stored into the ξ packages, respectively, according to the value of P_{ij}.

Step 3. A map is created with the same size of suspicious image and all its initial pixel values are set to zero.

Step 4. For each package PA_θ $(1 \le \theta \le \xi)$

Step 5. The block pairs contained in PA_θ will be matched according to their perceptual hash feature vectors and coordinate positions. The values of the corresponding coordinate positions in the map will be set to a same pixel value "255" according to the coordinates of the suspicious image if the block pairs are diagnosed as similar.

Step 6. For each block contained in package PA_θ, it will be matched with all blocks contained in package $PA_{\theta+1}$ if $1 \le \theta \le \xi - 1$ with the same method of Step 5.

Step 7. End For

Step 8. Outputting the map.

Algorithm 2: Similar region matching.

$P_{ij} = P_{mn}$ or $P_{ij} \approx P_{mn}$. Therefore, the perceptual hash feature vectors of blocks B_{ij} and B_{mn} will be stored into the same package PA_θ or two adjacent packages PA_θ and $PA_{\theta+1}$, where $\theta = (\lfloor P_{ij}/n \rfloor + 1)$ and $1 \le \theta \le \xi - 1$. Let the average pixel values of blocks B_{ij} and B_{mn} be $P_{ij} = 131$ and $P_{mn} = 132$, respectively. We have that the pixel mean range of package PA_{33} is $\{128, 129, 130, 131\}$ and the pixel mean range of package PA_{34} is $\{132, 133, 134, 135\}$. The two perceptual hash feature vectors of blocks B_{ij} and B_{mn} will be stored into the two adjacent packages. We need to match the perceptual hash feature vectors to diagnose the similar blocks in the same package and the adjacent package in the proposed similar region matching algorithm.

In Step 3, a map is created to mark the coordinate positions of all duplicated regions. It is the output in Algorithm 2. At the initial state, all of its values are set to zero. This means that there is no duplicated region at the initial state.

In Step 5, the similar image blocks that belong to the same package will be located according to their perceptual hash feature vectors and their actual coordinate distance. $\forall \theta \in \{1, 2, \ldots, \xi\}$, all perceptual hash feature vectors contained in package PA_θ will be compared with each other. Let B_{ij} and B_{mn} be two image blocks such that $B_{ij} \ne B_{mn}$, $F_{ij} = (P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4)$, and $F_{mn} = (P_{mn}, d_{mn}^1, d_{mn}^2, d_{mn}^3, d_{mn}^4)$ be their perceptual hash feature vectors, respectively, and $N \ge 0$ be a preset threshold. Blocks B_{ij} and B_{mn} can be considered as similar blocks if $\forall k \in \{1, 2, 3, 4\}$ such that $S(d_{ij}^k \oplus d_{mn}^k) \le N$, where $\oplus$ is an exclusive-OR operation for binary strings d_{ij}^k and d_{mn}^k and S is a function that is used to count the number of "1" in $d_{ij}^k \oplus d_{mn}^k$.

Specially, blocks B_{ij} and B_{mn} that are diagnosed as similar blocks should be excluded if their coordinate positions are adjacent in a suspicious image since the adjacent pixels of the suspicious image are generally smooth. Therefore, the coordinate distance of the two similar blocks B_{ij} and B_{mn} should be considered. Let (x_{ij}, y_{ij}) and (x_{mn}, y_{mn}) be the coordinates of blocks B_{ij} and B_{mn}, respectively. Their actual coordinate distance, denoted as α, can be calculated as follows:

$$\alpha = \sqrt{\left(x_{ij} - x_{mn}\right)^2 + \left(y_{ij} - y_{mn}\right)^2}. \tag{5}$$

If $\alpha > M$, similar blocks B_{ij} and B_{mn} are considered as actual similar blocks, where M is a preset threshold. If blocks B_{ij} and B_{mn} are diagnosed as actual similar blocks, the values of the coordinate positions (x_{ij}, y_{ij}) and (x_{mn}, y_{mn}), which are also the coordinate positions of similar blocks B_{ij} and B_{mn} in the suspicious image, should be marked with the same value, such as 255.

In Step 6, each block that belongs to package PA_θ will be matched with all blocks that belong to package $PA_{\theta+1}$ with the same method of Step 5 if $1 \le \theta \le \xi - 1$.

Let B_{ij} and B_{mn} be two image blocks and $F_{ij} = (P_{ij}, d_{ij}^1, d_{ij}^2, d_{ij}^3, d_{ij}^4)$ and $F_{mn} = (P_{mn}, d_{mn}^1, d_{mn}^2, d_{mn}^3, d_{mn}^4)$ be the perceptual hash feature vectors of B_{ij} and B_{mn}, respectively. We have $F_{ij} \approx F_{mn}$ if $B_{ij} \approx B_{mn}$, where $F_{ij} = F_{mn}$ is a particular case of $F_{ij} \approx F_{mn}$. It can be explained as follows. For blocks B_{ij} and B_{mn}, $\forall f_{ij}(x, y) \in B_{ij}$ and $\forall f_{mn}(x, y) \in B_{mn}$ such that $f_{ij}(x, y) \approx f_{mn}(x, y)$ if $B_{ij} \approx B_{mn}$, where $f_{ij}(x, y)$ (resp., $f_{mn}(x, y)$) represents the pixel of xth row and yth column in B_{ij} (resp., B_{mn}), we have $P_{ij} \approx P_{mn}$ since they are the pixel means of B_{ij} and B_{mn}, respectively.

Let C_{ij} and C_{mn} be the DCT coefficient matrixes of B_{ij} and B_{mn}, respectively. According to the independence and stability characteristics of DCT [21], we have $C_{ij} \approx C_{mn}$ if $B_{ij} \approx B_{mn}$. Naturally, we also have $C_{ij}^k \approx C_{mn}^k$, where C_{ij}^k and C_{mn}^k are the four subblocks of C_{ij} and C_{mn}, respectively, and $k \in \{1, 2, 3, 4\}$. Let m_{ij} and m_{mn} be the mean values of C_{ij}^1 and C_{mn}^1, respectively. We have $m_{ij} \approx m_{mn}$ since $C_{ij}^1 \approx C_{mn}^1$. Therefore, we have $H_{ij}^k \approx H_{mn}^k$ according to (3), where H_{ij}^k and H_{mn}^k are the perceptual hash matrixes of subblocks C_{ij}^k and C_{mn}^k, respectively. Note that H_{ij}^k and H_{mn}^k are two binary matrixes, which contain only "1" or "0." Automatically, we have $d_{ij}^k \approx d_{mn}^k$ since the decimal numbers d_{ij}^k and d_{mn}^k are uniquely computed from the two binary matrixes H_{ij}^k and H_{mn}^k, respectively. Therefore, we have $F_{ij} \approx F_{mn}$ since $P_{ij} \approx P_{mn}$ and $d_{ij}^k \approx d_{mn}^k$, where $k \in \{1, 2, 3, 4\}$. It indicates that

image blocks B_{ij} and B_{mn} may be a similar block pair if their perceptual hash feature vectors F_{ij} and F_{mn} are similar. In order to authenticate a suspicious image, we should detect all blocks of the suspicious image by comparing the perceptual hash feature vectors of these blocks.

3. Experiment and Analysis

In this section, the performance of the proposed scheme is tested and analyzed with many suspicious images that are involved in three image databases. The first one is the Columbia photographic images and photorealistic computer graphics database [22], which is made open for passive-blind image authentication research communities. In this database, about 1200 images are involved. We used Photoshop 8.0 to tamper images. All tampered suspicious images form the first experiment database. The second database contains two datasets MICC-F2000 and MICC-F220 that are introduced by Serra in [23]. The two datasets provide 1110 original images and 1110 tampered suspicious images with copy-move forgery. The original images contain animals, plants, men, artifacts, and natural environment. Moreover, to further evaluate the performance of the proposed scheme, 200 supplemented images are downloaded from the Internet and tampered with copy-move forgery to form the third database.

3.1. Evaluation Criteria Introduction. To evaluate the performance of copy-move forgery detection methods, researchers usually consider their test results at two different levels, that is, image level and pixel level [3]. At image level, it mainly focuses on the detection of whether an image is tampered or not. Let T_c be the number of tampered images that are correctly detected, F_c be the number of images that are erroneously detected to be the tampered images, and F_m be the number of falsely missed forgery images. The precision ratio p and recall ratio r [3] can be calculated by the following formulas:

$$p = \frac{T_c}{T_c + F_c} \times 100\%, \qquad r = \frac{T_c}{T_c + F_m} \times 100\%, \tag{6}$$

where the precision ratio p denotes the probability of a detected forgery being truly a forgery and the recall ratio r denotes the probability of a forgery being not missed.

At pixel level, it is used to evaluate the accuracy of duplicated regions. Let ω_s and ω_t be the pixels of an original region and a copy-move region in a suspicious image, respectively, and $\widetilde{\omega}_s$ and $\widetilde{\omega}_t$ be the pixels of an original region and a copy-move region in a detected result image, respectively. The detection accuracy rate (DAR) and false positive rate (FPR) are calculated as follows:

$$\mathrm{DAR} = \frac{|\omega_s \cap \widetilde{\omega}_s| + |\omega_t \cap \widetilde{\omega}_t|}{|\omega_s| + |\omega_t|} \times 100\%, \qquad \mathrm{FPR} = \frac{|\widetilde{\omega}_s - \omega_s| + |\widetilde{\omega}_t - \omega_t|}{|\widetilde{\omega}_s| + |\widetilde{\omega}_t|} \times 100\%, \tag{7}$$

where "||" means the area of region, "∩" means the intersection of two regions, and "−" means the difference of two regions. In this sense, the DAR shows the proportion of identified pixels that simultaneously belong to the really duplicated regions and all really duplicated pixels in all suspicious images. The FPR shows the ratio of some identified pixels that actually do not belong to the really duplicated regions and all identified pixels in all suspicious images. The four criteria indicate how precisely the proposed schemes can locate copy-move regions. Then, we can analyze the performance of the proposed scheme at the image level and the pixel level with the four criteria.

Table 1: Comparison of precision ratio p and recall ratio r.

Methods	[6]	[7]	[9]	[P]
Precision ratio (p)	0.865	0.896	0.822	0.902
Recall ratio (r)	0.900	0.850	0.864	0.910

Table 2: Parameters for the five kinds of attacks.

Attacks	Parameters
AWGN	SNR (10, 20, 30, 40, 50)
GB	ω (0.5, 1, 1.5, 2, 2.5)
ACR	gain (G) (0.3, 0.6, 0.9, 1.2, 1,5)
AL	bias (b) (3, 6, 9, 12, 15)
AH	H (5, 10, 15, 20, 25)

3.2. Effectiveness and Accuracy. In this experiment, 400 color images are selected to test the effectiveness and accuracy of the proposed scheme, including 100 original images, 100 forgery images, and other 200 images that are tampered with Photoshop 8.0. All tampered images do not suffer any postprocessing operation. Owing to space constrains, just a part of experimental results is shown in Figure 4. The DAR and FPR are calculated to illustrate the performance of the proposed scheme. In Figure 4, the DAR is generally greater than 0.85 and the FPR is also smaller. It indicates that the duplicated regions can be detected using the proposed scheme even though the duplicated regions are nonregular. Table 1 shows the comparison result of the proposed scheme and other existing schemes that are presented in [6, 7, 9]. It indicates that the p and r in the proposed scheme are better.

3.3. Robustness Test. In addition to the plain copy-move forgery, the detection for tampered images that are attacked by some postprocessing operations is also considered in the proposed scheme. Therefore, a series of experiments have been done to overall analyze the performance of the proposed scheme. It involves 1000 different suspicious images that come from the three databases. In this experiment, five kinds of attacks are considered, that is, adding white Gaussian noises (AWGN), adjusting contrast ratio (ACR), luminance (AL), hue (AH), and Gaussian blurring (GB), and their hybrid operations. Table 2 presents the parameters for the five kinds of attacks and Figure 5 shows a part of experimental results for the proposed scheme.

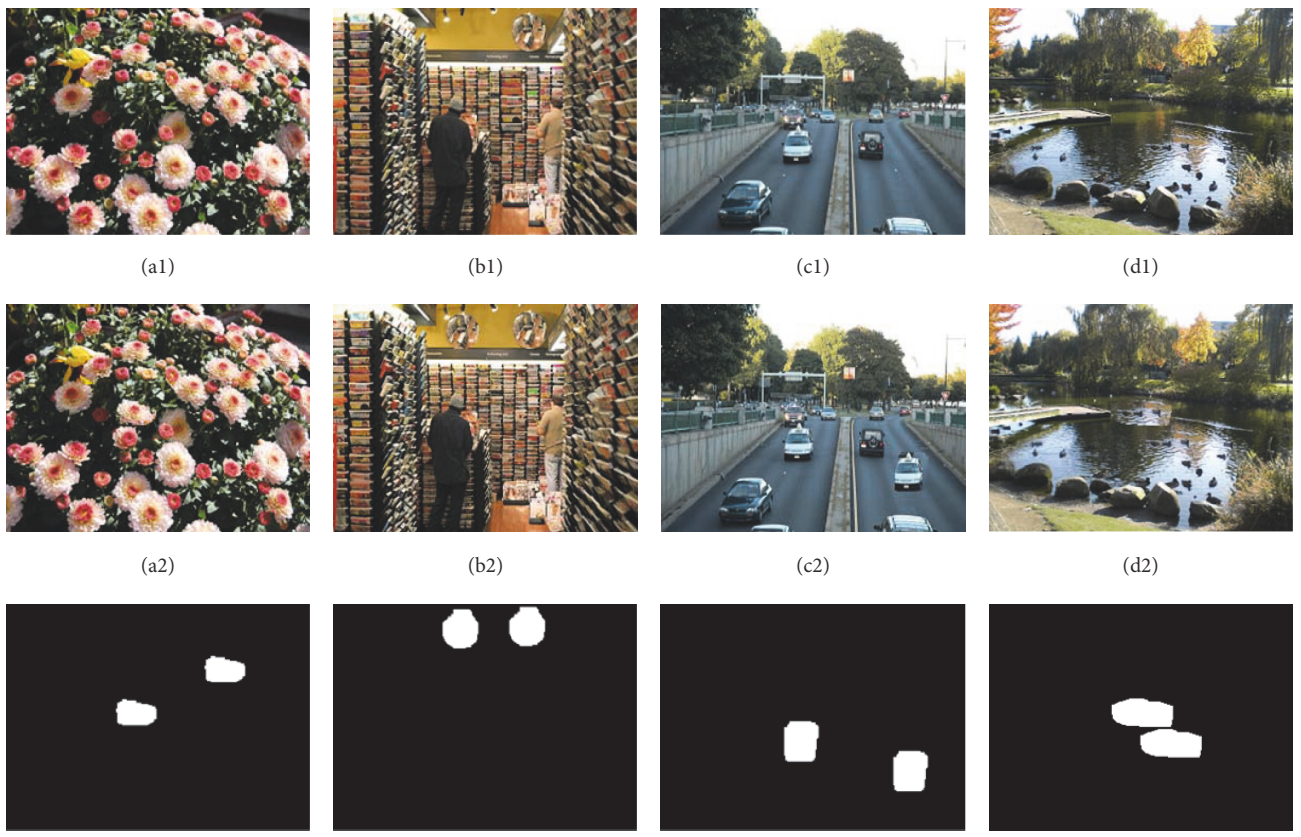

Figure 4: A part of experimental results for the proposed scheme. From top to bottom, the first row (a1)–(d1) shows the original images, the second row (a2)–(d2) shows the tampered images, and the last row (a3)–(d3) shows the detection results.

Table 3: Detection results for adding white Gaussian noise.

	SNR = 25	SNR = 35	SNR = 45
P	0.980	0.970	0.970
r	0.980	0.970	0.990
DAR	0.910	0.846	0.823
FPR	0.123	0.137	0.125

Table 4: Detection results for Gaussian blurring.

	$\omega = 1$	$\omega = 3$	$\omega = 5$
P	0.990	0.980	0.990
r	0.960	0.950	0.990
DAR	0.847	0.894	0.906
FPR	0.112	0.132	0.116

Table 5: Detection results for adjusting contrast ratio.

	$G = 0.9$	$G = 1.1$	$G = 1.4$
P	0.970	0.980	0.990
r	0.940	0.990	0.960
DAR	0.749	0.802	0.896
FPR	0.163	0.174	0.184

In this experiment, the proposed scheme is evaluated by DAR and FPR at the pixel level. The results indicate that the proposed scheme can locate multiple duplication regions although the suspicious images are attacked with different postprocessing operations.

In order to quantitatively evaluate the robustness of the proposed algorithm and analyze its ability to resist different image distortions, 100 tampered images are selected from the three databases. These tampered images are distorted by five kinds of attacks that are shown in Table 2. Then, there are 500 tampered images that will be detected in this experiment. For each kind of attacks, 100 tampered images are selected to be detected. Tables 3–7 show the detection results with the overall averages of p, r, DAR, and FPR. The robustness of the proposed scheme is evaluated at image level and pixel level.

Tables 3 and 4 show that the detection results of the proposed scheme are satisfactory for suspicious images that are attacked by adding white Gaussian noises and Gaussian blurring although the suspicious images have poor quality (SNR = 45 or $\omega = 5$). Only 14 images in all 600 tampered images are failed to be detected ($r = 0.9767$). The detection results of tampered images that are distorted by adjusting

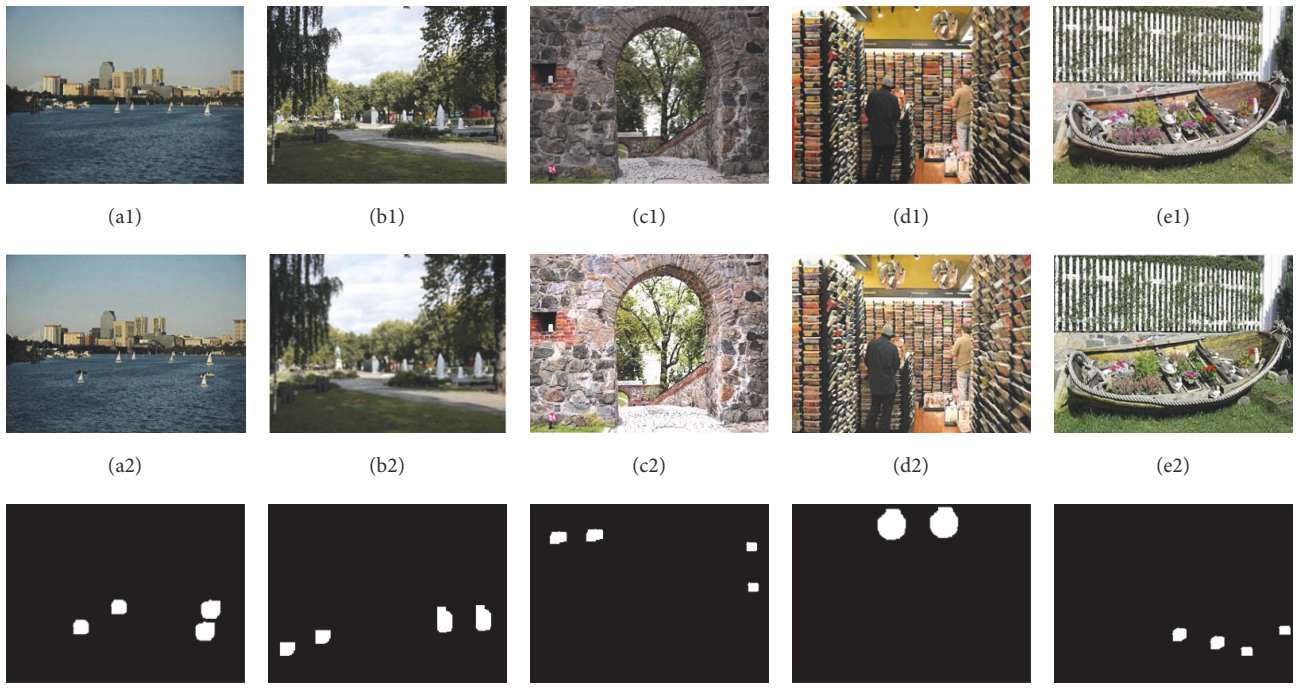

Figure 5: A part of the experimental results for the proposed scheme. From top to bottom, the first row (a1)–(e1) shows the five original images; the second row (a2)–(e2) shows the tampered images that are attacked with adding white Gaussian noises and Gaussian blurring, adjusting contrast ratio, luminance, and hue; the last row (a3)–(e3) shows the detection results of the proposed method.

Table 6: Detection results for adjusting luminance.

	$b = -3$	$b = 3$	$b = 10$
P	0.960	0.980	0.990
r	0.980	0.960	0.990
DAR	0.902	0.876	0.868
FPR	0.168	0.182	0.191

Table 7: Detection results for adjusting hue.

	$H = 10$	$H = 20$	$H = 30$
P	0.980	0.990	0.990
r	0.990	0.990	0.970
DAR	0.759	0.782	0.826
FPR	0.145	0.139	0.136

contrast ratio, luminance, and hue with different parameters are shown in Tables 5, 6, and 7, respectively. We can draw a conclusion from the three tables that the proposed scheme performs well also for attacks of adjusting contrast ratio, luminance, and hue.

3.4. Performances Comparison. In the last experiment, the performance of the proposed scheme is compared with other schemes presented in [6, 7, 9]. In this experiment, 400 tampered images are randomly selected from the three databases. They are tested by the proposed scheme and other schemes provided in [6, 7, 9], respectively. Figure 6 shows the performance comparison of these schemes with the overall averages of DAR and FPR for the 400 tampered images. We can see that the scheme proposed in [9] has the best detection results for the two kinds of attacks by adding white Gaussian noises and Gaussian blurring. However, its performance clearly drops down if the intensity of these attacks is gradually increased. Conversely, the proposed scheme is more robust for resisting various attacks. In most cases, the proposed scheme can also achieve better results for other three kinds of attacks with adjusting contrast ratio, luminance, and hue. Moreover, the proposed scheme has the lowest FPR results, which means that the proposed scheme can detect most duplicated regions in the selected suspicious images. The precision of the proposed scheme is higher than that obtained in [6, 7, 9].

The experimental results show that the proposed method can locate the tampered regions in a tampered image although it is distorted by some hybrid trace hiding operations, such as adding white Gaussian noise, Gaussian blurring, adjusting contrast ratio, luminance, and hue, and their hybrid operations. The proposed forensic technique can be used in politics, military, jurisprudence, and academic research. For example, a journalist takes a photo for a traffic accident. However, the journalist finds that the influence will be better if some crowds appear in this photo. Therefore, he

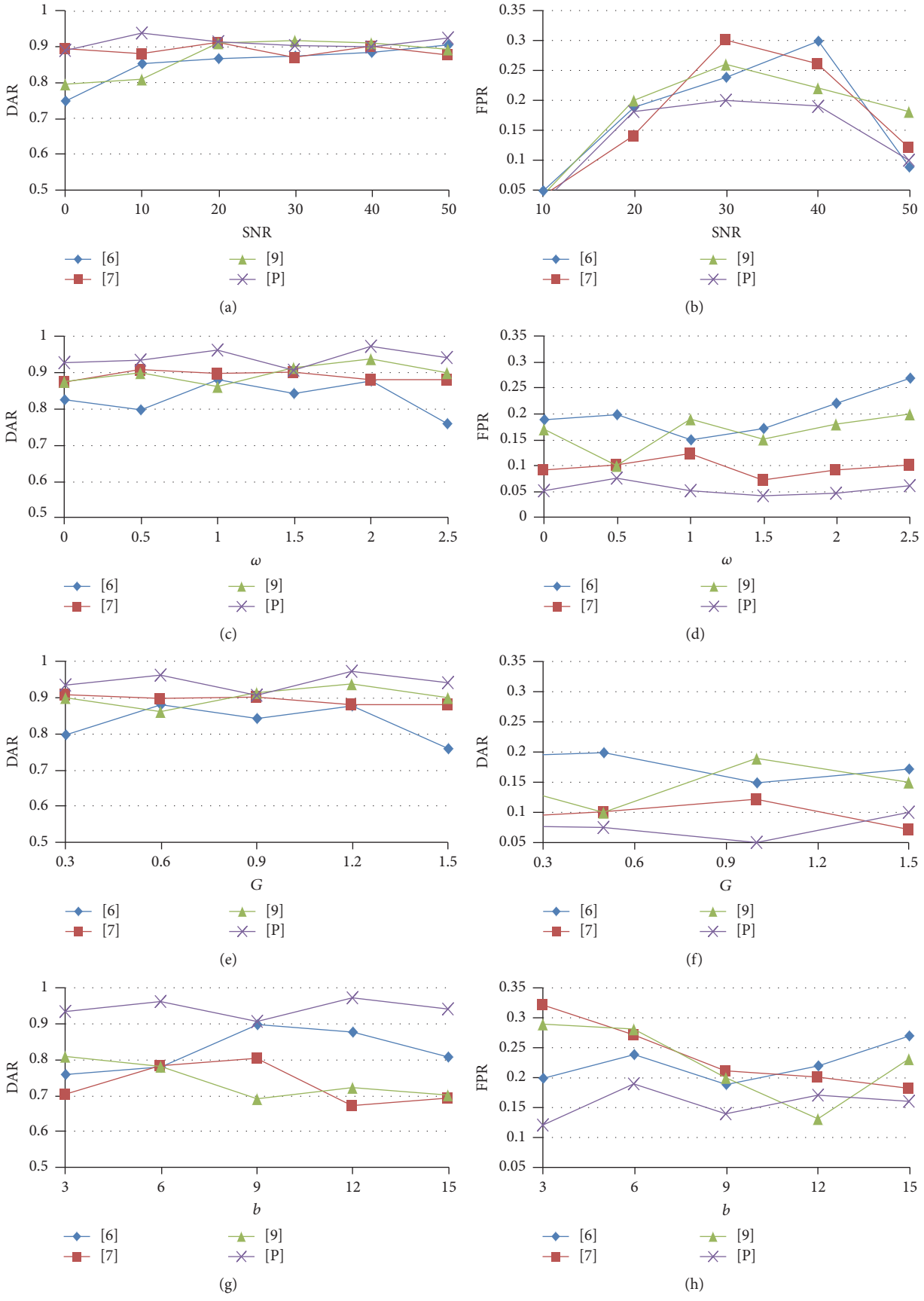

Figure 6: Continued.

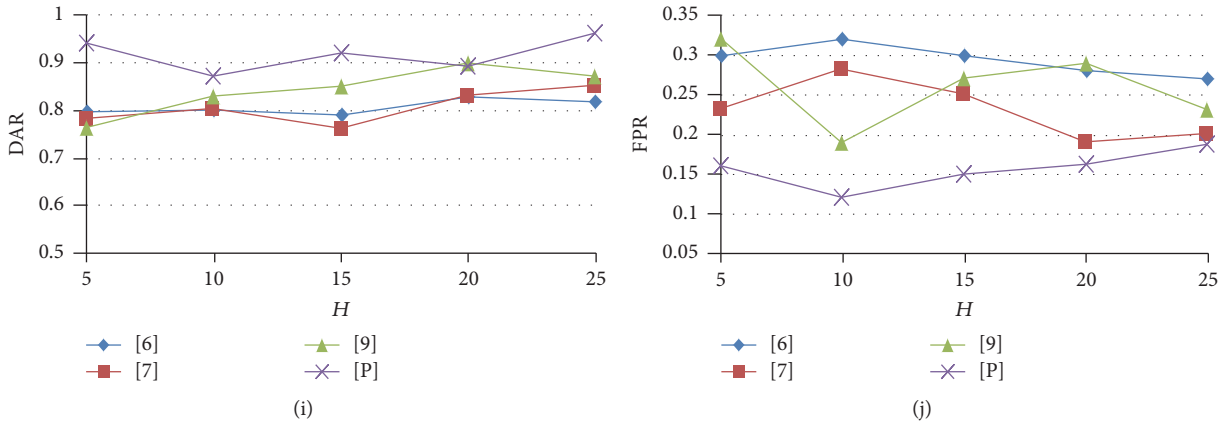

FIGURE 6: Comparison of different copy-move forgery schemes with 5 kinds of attacks. The two columns represent the result of DAR and FPR, respectively. (a), (b) Adding white Gaussian noise. (c), (d) Gaussian blurring. (e), (f) Adjusting contrast ratio. (g), (h) Adjusting luminance. (i), (j) Adjusting hue.

can use image processing tools to copy some people from the other side of this photo and paste them into the scene and use white Gaussian noise to conceal all tampering traces. Therefore, the authenticity of this traffic accident is broken. The news organization can detect this photo by using the proposed scheme to ensure its authenticity before this news is reported.

4. Conclusion

In this study, a passive authentication scheme is proposed based on perceptual hashing and package clustering algorithms to detect and locate the duplicated regions for copy-move forgery. The experiment results show that the proposed scheme based on perceptual hashing algorithms is robust for some special attacks, such as adjusting contrast ratio, luminance, and hue. A technology application of using perceptual hash strings to construct a feature vector to represent an image block can resist some conventional attacks, such as adding white Gaussian noises and Gaussian blurring. The proposed package clustering algorithm that is used to replace traditional lexicographic order algorithms can improve the performance of the proposed scheme. The evaluation criteria p, r, DAR, and FPR from the experiments show that the proposed scheme is better but the proposed scheme also has some weaknesses. For example, the time complexity is still unsatisfactory because of the previous image block dividing. Furthermore, the proposed scheme cannot resist some complex attacks, such as block rotation and scaling. In future work, we will focus on the studies of improving the time complexity and extending the robustness for more kinds of complex attacks, such as the rotation and scaling.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (NSFC) under Grant no. U1536110.

References

[1] J. Fridrich, D. Soukalm, and J. Lukas, "Detection of copy-move forgery in digital images," *Digital Forensic Research Workshop*, pp. 19–23, 2003.

[2] L. Kang and X. Cheng, "Copy-move forgery detection in digital image," in *Proceedings of the 3rd International Congress on Image and Signal Processing (CISP '10)*, pp. 2419–2421, Yantai, China, October 2010.

[3] 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, 2012.

[4] A. C. Popscu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2003-515, Dartmouth College, 2004.

[5] M. Babak and S. Stanislav, "Detection of copyCmove forgery using a method based on blur moment invariants," *IEEE Transactions on Information Forensics*, vol. 10, no. 3, pp. 507–518, 2007.

[6] Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm fosr region duplication in digital images," *International Journal of Digital Content Technology and its Applications*, vol. 5, no. 6, pp. 95–103, 2011.

[7] S. A.-N. Thajeel and G. Sulong, "A novel approach for detection of copy move forgery using completed robust local binary pattern," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 2, pp. 351–364, 2015.

[8] H. Wang, H.-X. Wang, X.-M. Sun, and Q. Qian, "A passive authentication scheme for copy-move forgery based on package clustering algorithm," *Multimedia Tools and Applications*, vol. 76, no. 10, pp. 12627–12644, 2017.

[9] J. Zhong, Y. Gan, J. Young, L. Huang, and P. Lin, "A new block-based method for copy move forgery detection under image geometric transforms," *Multimedia Tools and Applications*, vol. 76, no. 13, pp. 14887–14903, 2017.

[10] R. Dixit, R. Naskar, and S. Mishra, "Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD," *IET Image Processing*, vol. 11, no. 5, pp. 301–309, 2017.

[11] X. L. Bi and C. M. Pun, "Fast reflective offset-guided searching method for copy-move forgery detection," *Information Sciences*, pp. 531–545, 2017.

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

[13] I. Amerini, M. Barni, R. Caldelli, and A. Costanzo, "Counter-forensics of SIFT-based copy-move detection by means of keypoint classification," *EURASIP Journal on Image and Video Processing*, pp. 1–17, 2013.

[14] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507–518, 2015.

[15] X. Wang, G. He, C. Tang, Y. Han, and S. Wang, "Keypoints-Based Image Passive Forensics Method for Copy-Move Attacks," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 30, no. 3, Article ID 1655008, 2016.

[16] J. Li, F. Yang, W. Lu, and W. Sun, "Keypoint-based copy-move detection scheme by adopting MSCRs and improved feature matching," *Multimedia Tools and Applications*, vol. 76, no. 20, pp. 20483–20497, 2017.

[17] X.-Y. Wang, S. Li, Y.-N. Liu, Y. Niu, H.-Y. Yang, and Z.-L. Zhou, "A new keypoint-based copy-move forgery detection for small smooth regions," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 23353–23382, 2017.

[18] X. M. Niu and Y. H. Jiao, "An overview of perceptual hashing," *ACTA Electronica Siniica*, vol. 36, no. 7, pp. 1405–1411, 2008.

[19] W. Johannes, "Detecting visual plagiarism with perception hashing," *Degree Project in Computer science*, 2015.

[20] Z. Yin, X. Niu, Z. Zhou, J. Tang, and B. Luo, "Improved Reversible Image Authentication Scheme," *Cognitive Computation*, vol. 8, no. 5, pp. 890–899, 2016.

[21] E. Y. Lam and J. W. Goodman, "A mathematical analysis of the DCT coefficient distributions for images," *IEEE Transactions on Image Processing*, vol. 9, no. 10, pp. 1661–1666, 2000.

[22] T. T. Ng, S. F. Chang, J. Hsu, and M. Pepeljugoski, Columbia photographic images and photorealistic computer graphics dataset ADVENT, Columbia University, New York, NY, USA, 2004.

[23] G. Serra, "A SIFT-based forensic method for copy-move detection. Giuseppe Serra 2014," http://giuseppeserra.com/content/sift-based-forensic-method-copy-move-detection.