Exposing Image Forgery by Detecting Traces of Feather Operation

Jiangbin Zheng, Tingge Zhu , Zhe Li
Dept. of Computer Science and Engineering, School of Computer, Northwestern Polytechnical University
Xi'an, China
zhengjb0163@163.com

Weiwei Xing
School of Software Engineering, Beijing Jiaotong University
Beijing, ,China
wwxing@bjtu.edu.cn

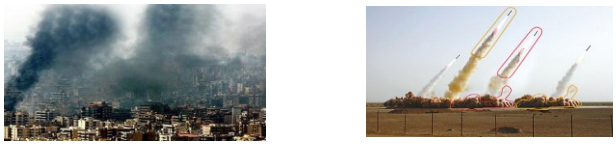
JinChang Ren
Dept. of Electronic and Electrical Engineering, University of Strathclyde Glasgow
G1 1XW, United Kingdom
jinchang.ren@strath.ac.uk

***Abstract*—Powerful digital image editing tools make it very easy to produce a perfect image forgery. The feather operation is necessary when tampering an image by copy-paste operation because it can help the boundary of pasted object to blend smoothly and unobtrusively with its surroundings. We propose a blind technique capable of detecting traces of feather operation to expose image forgeries. We model the feather operation, and the pixels of feather region will present similarity in their gradient phase angle and feather radius. An effectual scheme is designed to estimate each feather region pixel's gradient phase angle and feather radius, and the pixel's similarity to its neighbor pixels is defined and used to distinguish the feathered pixels from un-feathered pixels. The degree of image credibility is defined, and it is more acceptable to evaluate the reality of one image than just using a decision of YES or NO. Results of experiments on several forgeries demonstrate the effectiveness of the technique.**

Keywords-Tampered image; image forgery; feather operation; tampering detection.

I. INTRODUCTION

With the great increasing usage of digital photography and the advancing of new technologies, powerful image editing software make it very easy today to create a believable image forgery even for a non-specialist. Today more and more images of high quality are presented on screen. It challenges our ability to tell what's real and what's not. Some samples of image forgeries obtained over the internet are shown in Fig.1.



(a) (b)

Fig.1.Examples of image forgeries obtained from internet (a) the published Reuters photograph showing the remnants of an Israeli bombing. (b) the published photograph showing four Iranian missiles streaking skyward.

In August of 2006, the Reuters news agency published a photograph [Fig.1.(a)] showing the remnants of an Israeli bombing of a Lebanese town, and in the week that followed, the photograph was revealed by nearly every major news organization to have been doctored with additional more smoke. An example of photo tampering came to light in July 2008. A photograph [Fig.1.(b)] showing four Iranian missiles streaking skyward was first posted on the Web site of Sepah News, the media arm of Iran's Revolutionary Guard. But only three of those rockets actually left the ground; the fourth was digitally added.

The appearance of more and more artificial images has broken up people's long-term confidence on the reality of image. Image authentication plays an important role in people's lives, and it's significant in many social areas such as forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, medical imaging and journalism. As a consequence, we should pay special attention to the field of image authenticity.

In fact, there are no universally applicable solutions due to multifarious tampering means. Vast observation suggests that the feather operation is nearly inevitably in tampering. A novel approach to expose image forgeries is presented in this paper. It works by determining if feather operation was used at the edge of one object and locating the traces of feather operation. In comparison with the previous work, it is computationally much simpler and does not require a large image database to train a classifier. What's more, the degree of image credibility is defined in our scheme to judge the reality of an image. We think it more acceptable than just using a decision of yes or no.

The steps of the algorithm proposed in this paper can be summarized as follows and the flow chart is shown in Fig.2.

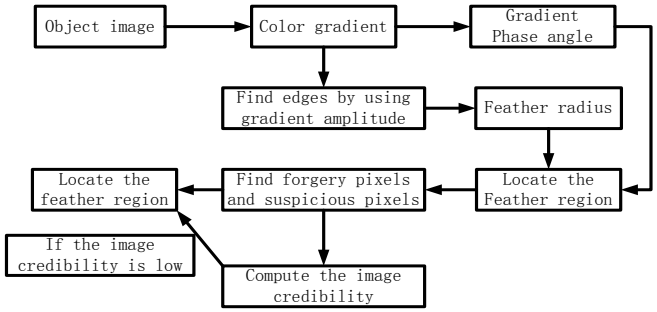


Fig.2 The flow chart of exposing image forgeries by detecting traces of feather operation

a) Find the image's edge by using color gradient amplitude $F(\theta)$, and get the gradient phase angle θ.

b) Estimate the feather radius r for every edge pixels.

c) Estimate the similarity s_q for each edge pixel by using r_q and θ_q, and find the feathered pixels.

d) Locate the forgery region and compute the degree of image credibility.

This paper is organized as follows. The related prior work is summarized in section 2. The most common tampering steps and models of the feather operation are given in section 3. In section 4 and 5, we demonstrate the influence of the feather operation on the gradient phase angle and the feather radius for edge pixels. In Section 6, we explain how to compute the degree of image credibility and how to locate the feather regions. In section 7, we show the experimental results of the proposed algorithm. Finally, the conclusion is made in Section 8.

II. RELATED PRIOR WORK

Digital watermarking has been proposed as an active approach for providing image authenticity [1]. The drawback of this approach is that a watermark must be inserted when the image is created. Although image forgeries may leave no visual clues, they may alter the underlying statistics of an image by which we may detect suspicious images. These detecting methods are passive techniques. Recently, the state-of-the-art digital image forensics in the context of three predominant types of forensic are presented in [2] by Tanzeela Qazi, which include copy or move forgery, image splicing and image retouching.

We classify the passive techniques for image forensics into three categories according to different forensic features: techniques based on the traces left by the tampering process, techniques based on the consistency of imaging equipment, and techniques based on the statistical characteristics of natural images. We will review some typical forensic techniques within each category as follows.

2.1 Techniques based on the traces left by tampering process.

One of the common image tampering is to copy and paste portions of the image to conceal a person or object in the scene. The presence of copy-paste region can be the evidence of tampering [3][4]. In [3] and [4], the image is divided into fixed-size overlapping blocks whose features are represented by the discrete cosine transform (DCT) coefficients. Feature dimension reduction is different from them. Truncating is used to reduce it in [3], however in [4] each block represented by the quantized DCT coefficients is divided into non-overlapping sub-block, the dimension of the SVD (singular value decomposition) based features from each quantized block is reduced by largest singular value. Then the duplicated regions were detected by lexicographically sorting the features vectors and two similar feature vectors are exported. This approach in [5] was available whether the copied area came from the same image or not, if only source image was JPEG compressed. For JPEG format images, it is likely that the manipulated image is compressed twice, and the double compression introduces specific artifacts not present in singly compressed images. Thus, the presence of these artifacts can be the evidence of tampering [6] [7]. H. Farid described a technique [8] to expose JPEG ghosts by detecting whether part of an image was initially compressed at a lower quality than the rest of the image. The re-sampling operations [9][10] are often necessary in tampering, and these operations can introduce specific periodic correlations between neighboring pixels, which can be used to detect tampering. When creating a composite of two or more images, it is often difficult to exactly match the lighting, thus, the lighting inconsistencies can be a useful tool for revealing traces of digital tampering. These methods presented in [11] can detect doctored image based on consistency of shadow. In [12], the authors described how to estimate a camera's principal point form the image of a pair of eyes or other planar geometric shapes. They showed how translation in the image plane was equivalent to a shift of the principal point. Inconsistencies in the principal point across an image were then used as evidence of tampering. The authors in [13] proposed a method to detect image tampering operations that involved sharpness/blurriness adjustment, and the estimate of sharpness/blurriness value was based on the regularity properties of wavelet transform coefficients. The method proposed in [14] can detect image splicing by evaluating inconsistencies in motion blur. In [15], we proposed a technique based on the local entropy of the gradient to detect the image forgery, and it can discover the traces of artificial feather operation. In [16], we proposed a technique based on the wavelet holomorphic filtering to recognize some traces of artificial blur operation.

2.2 Techniques based on the consistency of imaging equipment.

When an image is created, the characters brought by imaging equipment should present consistence in the whole natural image, which can be used as evidence of tampering. The common methods include: CFA interpolation detection, sensor noise detection, chromatic aberration detection and camera response detection.

The presence of lack of correlations produced by CFA interpolation can be used to authenticate an image. The algorithm described in [17] can detect image forgery by estimating color modification in images. The authors in [18] proposed a method base on the observation that each in-camera and post-camera processing operation left some distinct intrinsic fingerprint traces on the final image. They characterized the properties of a direct camera output using a camera model [19], and considered any further post-camera processing as a manipulation filter. The method could be used to verify whether a given digital image was a direct camera output and identified different types of post-camera processing. The authors in [20] modeled camera processing with an additive and multiplicative noise model. The parameters of the noise model were estimated from the original camera or a series of images originating from the known camera. Correlations between the estimated camera noise and the extracted image noise were then used to authenticate an image. The authors in [21] modeled the camera processing with a generic additive noise model and used statistics from the estimated noise for image forensics. M.K.Johnson and H.Farid in [22] indicated that the chromatic aberration resulted from the failure of an optical system to perfectly focus light of different

wavelengths, and these aberrations could be used to detect digital tampering by approximated with a low-parameter model. They developed an automatic technique for estimating the model parameters that was based on maximizing the mutual information between color channels. The authors [23] described how to estimate the mapping, termed a response function, from a single image. The differences in the response function across the image were then used to detect tampering. An automatic splicing detection is proposed in [24], which is based a rigorous camera response function (CRF) consistency checking principle.

2.3 Techniques based on the statistical characteristics of natural images.

Natural images are not simply a collection of independent pixels. The visual structures making them look "natural" are the result of strong correlations among pixels. The techniques in this category try to model statistical regularities within natural image, which is used to discriminate photographic from computer-generated images or tampered ones and to detect hidden messages. Wei Lu [25] proposes a detection scheme for natural images and fake images, in which the support vector machine (SVM) is used to differentiate true and faked images by the extracted feature using multi-resolution decomposition and higher order local auto correlations (HLACs). The authors in [26] developed an image forensic scheme based on the interplay between feature fusion and decision fusion. The authors in [27] proposed a method for digital image forensics based on Binary Similarity Measures between bit planes used as features. The basic idea was that the correlation between the bit planes as well as the binary texture characteristics within the bit planes would differ between an original and a doctored image. This change in the intrinsic characteristics of the image could be monitored via the quintal-spatial moments of the bit plants.

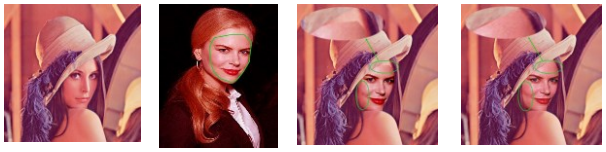
III. THE FEATHER OPERATION MODEL

One of the most common image manipulations is to copy and paste part of one image to another one. This operation can conceal or add an important person or object in the scene. When this is done, it seems to be potentially discontinuous or obtrusive along the boundary of the pasted region. The feather operation is necessary, and it helps to create a smooth transition between the pasted region and its surroundings. The common method to produce a fake image is shown in Fig.3, in which we can create an image forgery by using feather operation, and it can weaken the traces of splicing.

When a region of one image is copy-pasted to another one, new edge with step shape will incur naturally as shown (c) in Fig.3. New edge $f(x)$ without any post-processing can be simulated by Eq. (1), and the width of the new edge is 0 pixel (Fig.4).

$$f(x)=\begin{cases} Q_1, & x=A \\ Q_2=Q_1+H, & x=A+1 \end{cases} \tag{1}$$

Where, $x=A$ denotes the position of the new edge, Q_1 and Q_2 denote the edge pixel values of the background and the pasted region, H denotes the offset.



(a) (b) (c) (d)

Fig.3. Example for the most common image manipulations to create an image forgery. (a) is the original Lena image, (b) is the photo of Nicole Mary Kidman. (c) is a composite image forgery by copying Nicole Mary Kidman's face to Lena image. (d) is another composite image forgery, in which the traces of splicing around the face are not clear due to the feather operation.

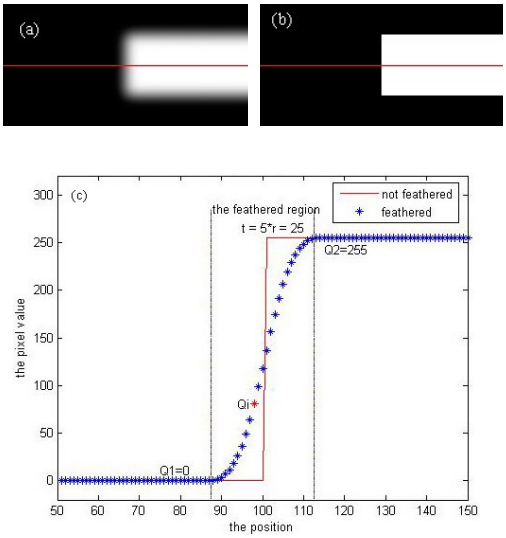


Fig.4. Feathered image (a) and un-feathered edge (b). Profile of the red line in (c) to show the difference between the feathered edge and un-feathered edge.

Given the specified feather radius r, the feather operation can make a smooth transition between Q_1 and Q_2, and create a new edge with the width of t pixels $(t>0)$. The effect of feather operation is shown in Fig.4.

We have made statistical analysis for the relationship between the new edge's width t and the feather radius r. The relationship between r and t is shown in Fig.5, which approximately satisfies $t=5r$. So the new edge after the feather operation will become wider to make a smooth transition in the feather region.

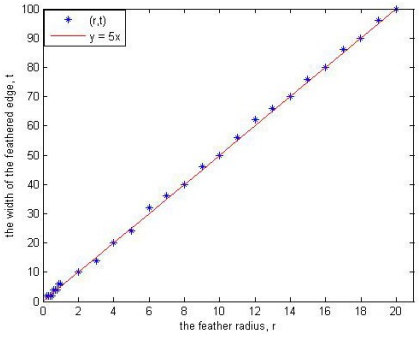


Fig.5. The relationship between t and r

It suggests that each pixel Q_i in the feather region is acquired via the interpolation between the pixel Q_1 of the

background and the pixel Q_2 of the pasted object through vast observation for the feather data. Thus the model of feather operation is described as follows:

$$Q_i = (1-\frac{i}{5r})Q_1 + \frac{i}{5r}Q_2 \qquad i \in \{0,1,...,5r\} \qquad (2)$$

Then the new edge after the feather operation can be described by Eq.(3)

$$f'(x) = \begin{cases} Q_1, & x = A - 2.5r \\ (1-\frac{x+2.5r}{5r})Q_1 + \frac{x+2.5r}{5r}Q_2, & A-2.5r < x < A+2.5r \\ Q_2 = Q_1 + H, & x = A+2.5r \end{cases} \qquad (3)$$

With the increasing of feather radius *r*, the new edge $f'(x)$ with feather operation will become wider and smoother. It is obvious that the new edge $f'(x)$ is a line function of *x* from Eq.(3), its slope is defined as the feather slope *k*, which describes the speed of smooth transition in the feather region. With the decreasing of *k*, the transition will become smoother, and vice versa.

$$k = \frac{Q_2 - Q_1}{5r} \qquad (4)$$

Thus, the feather radius can be estimated by Eq.(5) :

$$r = \frac{Q_2 - Q_1}{5k} = \frac{H}{5k} \qquad (5)$$

The accuracy of estimation of feather radius *r* is directly determined by the feather slope *k*. Then we will demonstrate how to measure the value of *k* in section 5.

IV. THE GRADIENT OF COLOR IMAGE

The derivative or the first difference of a linear function is a constant at every position. Based on the model of feather operation, the gradient in feather region will present smooth. An example of the influence of feather operation on the gradient phase angle is shown in Fig.6. As shown in (e) and (f), the gradient phase angle of the yellow flower's boundary present smooth due to the feather operation. Thus the smooth feature of the gradient phase angle can be used to expose the traces of feather operation.

Our interest is in computing the gradient in RGB color space. The way for RGB images would be computing the gradient of each color component and then combining the results. Unfortunately, in consideration of the dependence among the three channels, the gradient using this method is always undesirable. We define one pixel in a color image as a vector, and compute the gradient by extending the concept of gradient from scalar function to vector function. Let $\mathbf{r},\mathbf{g},\mathbf{b}$ be unit vectors along the R, G, B axis of RGB color space, and define the vectors

$$\mathbf{u} = \frac{\partial R}{\partial x}\mathbf{r} + \frac{\partial G}{\partial x}\mathbf{g} + \frac{\partial B}{\partial x}\mathbf{b} \qquad (6)$$

$$\mathbf{v} = \frac{\partial R}{\partial y}\mathbf{r} + \frac{\partial G}{\partial y}\mathbf{g} + \frac{\partial B}{\partial y}\mathbf{b} \qquad (7)$$

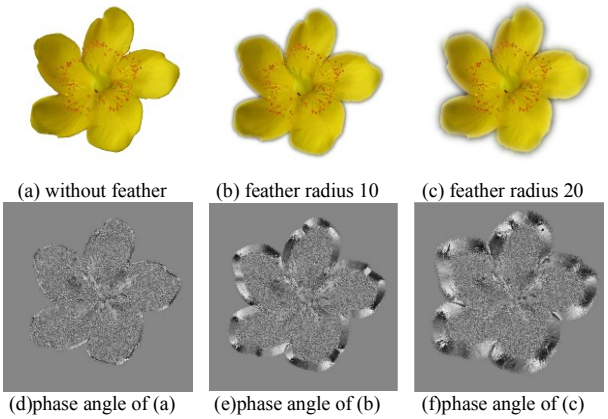


Fig.6. The influence of feather operation on the phase angle. Shown in the first row from left to right are the original image (a), the forgeries with feather radius $r = 10$ (b) and $r = 20$ (c). Shown in the second row are the gradient phase angle images respectively

Let the quantities g_{xx}, g_{yy} and g_{xy} be defined in terms of the dot product of these vectors as follows:

$$g_{xx} = \mathbf{u} \bullet \mathbf{u} = \mathbf{u}^T\mathbf{u} = \left|\frac{\partial R}{\partial x}\right|^2 + \left|\frac{\partial G}{\partial x}\right|^2 + \left|\frac{\partial B}{\partial x}\right|^2 \qquad (8)$$

$$g_{yy} = \mathbf{v} \bullet \mathbf{v} = \mathbf{v}^T\mathbf{v} = \left|\frac{\partial R}{\partial y}\right|^2 + \left|\frac{\partial G}{\partial y}\right|^2 + \left|\frac{\partial B}{\partial y}\right|^2 \qquad (9)$$

$$g_{xy} = \mathbf{u} \bullet \mathbf{v} = \mathbf{u}^T\mathbf{v} = \frac{\partial R}{\partial x}\frac{\partial R}{\partial y} + \frac{\partial G}{\partial x}\frac{\partial G}{\partial y} + \frac{\partial B}{\partial x}\frac{\partial B}{\partial y} \qquad (10)$$

R, G, B and consequently the g's, are functions of *x* and *y*. Using this notation, it can be shown in [28] that the direction of maximum rate of change of $\theta(x,y)$ as a function (x,y) is given by the angle

$$\theta(x,y) = \frac{1}{2}\arctan\left[\frac{2g_{xy}}{g_{xx} - g_{yy}}\right] \qquad (11)$$

and that the value of the rate of change (i.e., the magnitude of the gradient) in the directions given by the elements of $\theta(x,y)$ is given by

$$F_\theta(x,y) = \left\{\frac{1}{2}\left[(g_{xx}+g_{yy}) + 2g_{xy}\sin 2\theta + (g_{xx}-g_{yy})\cos 2\theta\right]\right\}^{1/2} \qquad (12)$$

Note that $\theta(x,y)$ and $F_\theta(x,y)$ are images of the same size as the input image. The elements of $\theta(x,y)$ are simply the

angles at each point that the gradient is calculated, and $F_\theta(x,y)$ is the gradient image.

V. ESTIMATE THE FEATHER RADIUS

The feather radius is set by the forgery when the feather operation is used, and it is a constant in the same feather region. So we estimate the feather slope by using the least square method, and then compute the feather radius. Based on our model, the pixels in feather region will satisfy a line relationship. We define 16 directions around one pixel, and find the feather direction by detecting if the pixels along the direction can be best fitted by a line function. The feathered pixels along the feather direction can be used to estimate the feather slope.

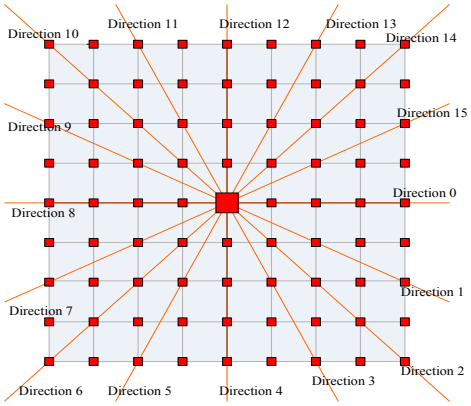


Fig.7. The 16 directions around the center pixel.

We define a neighborhood Ω size of $2.5r$ and 16 directions D_j around the pixel q as shown in Fig.7.

$$D_j = j\pi/8, \quad j = 0,1,...,15$$

There are $5r+1$ pixels along direction D_j, and the pixel values are $y_{-2.5r}$, $y_{-2.5r+1},...,y_{2.5r-1}$, $y_{2.5r}$. We assume that the relationship of the pixel values is well represented by a linear function as shown in Eq.(13) by using the least square method.

$$y = kx + b \; x \in \{-2.5r, \; -2.5r+1,...,0,...,2.5r-1, \; 2.5r\} \quad (13)$$

Where, k is the slope, b is the intercept, y represent pixel values, and x is the position. The slope k is different from the direction D_j. D_j is a direction in a horizontal plane, and k is the slope of the linear function. The slope k and the intercept b of the linear function can be estimated by Eq.(14) and (15).

$$\hat{k}_{D_j} = \frac{(5r+1)(\sum x_i y_i) - (\sum x_i)(\sum y_i)}{(5r+1)(\sum x_i^2) - (\sum x_i)^2} \quad (14)$$

$$\hat{b}_{D_j} = \frac{(\sum x_i^2)(\sum y_i) - (\sum x_i)(\sum x_i y_i)}{(2r+1)(\sum x_i^2) - (\sum x_i)^2} \quad (15)$$

Where $\sum$ is equal to $\sum_{i=-2.5r}^{2.5r}$. The correlation coefficient R_{D_j} can be defined as followed.

$$R_{D_j} = \frac{\sum_{i=-2.5r}^{2.5r}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=-2.5r}^{2.5r}(x_i - \bar{x})^2}\sqrt{\sum_{i=-2.5r}^{2.5r}(y_i - \bar{y})^2}} \quad (16)$$

Because $x \in \{-2.5r, \; -2.5r+1,...,0,...,2.5r-1, \; 2.5r\}$, then $\bar{x} = 0$, the Eq.(16) can be rewritten as Eq.(17).

$$R_{D_j} = \frac{\sum_{2.5i=-r}^{2.5r} x_i(y_i - \bar{y})}{\sqrt{\sum_{i=-2.5r}^{2.5r} x_i^2}\sqrt{\sum_{i=-2.5r}^{2.5r}(y_i - \bar{y})^2}} \quad (17)$$

Where,

$$\bar{y} = \frac{1}{5r+1}\sum_{i=-2.5r}^{2.5r} y_i, \quad (18)$$

The correlation coefficient has a range of $R_{D_j} \in [-1,1]$. With the increasing of $|R_{D_j}|$, the linearity between x and y gets more consummate, and vice versa.

The standard deviation S_{D_j} can be computed in the following way as show in Eq.(19)..

$$S_{D_j} = \sqrt{\frac{1}{5r+1-2}\sum_{i=-2.5r}^{2.5r}[y_i - (\hat{k}\,x_i + \hat{b})]^2} \quad (19)$$

If $S_{D_j} = 0$, the straight line fits perfectly, namely, every pixel point lies on the straight line. With the increasing of S_{D_j}, the fit will get worse, because the deviations of points from the straight line become larger.

For all the directions $D_j, j = 0,1,...,15$, we compute the slope $\hat{k}_{D_j}$, the correlation coefficient R_{D_j}, and the standard deviation S_{D_j} respectively. If the value of S_{D_j} is minimum, and $S_{D_j} < \gamma_1$, $|R_{D_j}| > \gamma_2$, we consider the direction D_j as the feather direction, and the slope $\hat{k}_{D_j}$ as the feather slope k.

$$k = \hat{k}_{D_j}, \quad \text{if } S_{D_j} < \gamma_1 \text{ and } |R_{D_j}| > \gamma_2 \quad (20)$$

Where, γ_1 and γ_2 are two thresholds, which are determined by lots of experiments. When the condition of Eq.(20) is satisfied, k is estimated by Eq.(14), then the feather radius can be estimated by Eq.(5), in which H is an empirical offset.

Conversely, if the condition is not satisfied, k and r are not estimated. It means this region is not tampered.

VI. DETECTION OF THE FORGERIES

The presence of feather operation can be used as the evidence of tampering. So, in this section, we detect the traces of feather operation by using the smoothness of the gradient phase angle and uniformity of the feather radius. The degree of image credibility is defined to describe the reality of one image.

Let $q(m,n)$ denote one pixel, and Ω is its neighborhood. The most common neighborhood can be defined as shown in Fig.7.

$$q(m \pm i, n \pm j) \in \Omega \quad (\mathrm{i,j} = 0, \ldots, 5) \tag{21}$$

The similarity of pixel q among its neighbor pixels can be calculated by the following way.

$$s_q = \alpha \times r_q + \beta \times \theta_q \tag{22}$$

Where, α and β are weight coefficients. r_q and θ_q are defined as follows.

$$r_q = \frac{\sum_{q_i \in \Omega} C_r(q, q_i)}{N} \tag{23}$$

$$\theta_q = \frac{\sum_{q_i \in \Omega} C_\theta(q, q_i)}{N} \tag{24}$$

Where, N is the total number of pixels in the neighborhood Ω. $C_r(q,q_i)$ and $C_\theta(q,q_i)$ are defined as follows.

$$C_r(q,q_i) = \begin{cases} 1, & \text{if } \left| r_q - r_{q_i} \right| \le \lambda_r \\ 0, & \text{if } \left| r_q - r_{q_i} \right| > \lambda_r \end{cases} \tag{25}$$

$$C_\theta(q,q_i) = \begin{cases} 1, & \text{if } \left| \theta_q - \theta_{q_i} \right| \le \lambda_\theta \\ 0, & \text{if } \left| \theta_q - \theta_{q_i} \right| > \lambda_\theta \end{cases} \tag{26}$$

Where, q_i is a neighbor pixel in the neighborhood Ω of q, r_q is an approximate calculation of feather radius, θ_q is a phase angle of the gradient at q. In the neighborhood Ω, $C_r(q,q_i)$ denotes number of pixels which are similar to feather radius at q, and $C_\theta(q,q_i)$ denotes number of pixels which are similar to the phase angle of the gradient at q.

For a pixel q, if $s_q \ge \delta_s$, we mark q as the feathered pixel, if $s_q \ge \delta_s - \mu$, we mark q as the suspicious pixel, where δ_s and μ are thresholds.

Let N_f and N_s denote the number of feathered pixels and suspicious pixels. That is to say:

$$\begin{cases} \text{if } s_q \ge \delta_s & \text{then } N_f + 1 \\ \text{if } s_q \ge \delta_s - \mu & \text{then } N_s + 1 \end{cases} \tag{27}$$

The degree of image credibility can be defined as Eq.(28). We think it more acceptable to judge the reality of one image than just using a decision of YES and NO, which is usually used in many existing works.

$$D_{credibility} = 1 - \frac{N_f}{N_s} \tag{28}$$

The feathered pixels are marked with 255 and others with 0, and the result is presented by a binary image. We process the binary image using erosion and dilation operations to remove the isolated points and make the density points conjoined. If a connected region or a meaningful region can be structured by the white points, we regard it as the suspicious feather region.

VII. RESULTS

(1) Image database

In order to make experiment convenient, we have employed some students, who are unaware of our detection method, to build a database (more than 4000 images) for us. A set of image forgeries undergone the feather operation with various feather radius by using photo-shop have been chosen from our database to test the efficacy of our proposed algorithm. These images span a wide range of indoor and outdoor scenes. Most of them are captured in real scene by several digital cameras (including SONY DSC-T200, Olympus E20，Sony DSC-W220, Cannon 450D, Cannon D40 and Panasonic FS7GK), the rest a few are downloaded from the internet according to the need. They are saved in the JPEG format at the same or different quality. Fig.8 shows some representative examples used in our experiment.

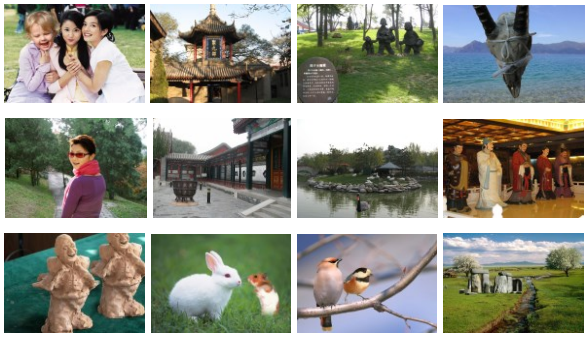


Fig.8. Some representative test images.

(2) Experiment results

In our experiment, 120 images are chosen to test our algorithm. Tab.1 shows the successful rate, from which we can see that our algorithm is effective to detect the traces of feather operation without reference to the feather radius. The degree of image credibility for the test images are showed in Fig.9, from

which we can see that the credibility of original image is usually higher than 85%, and the credibility of forgery is much lower.

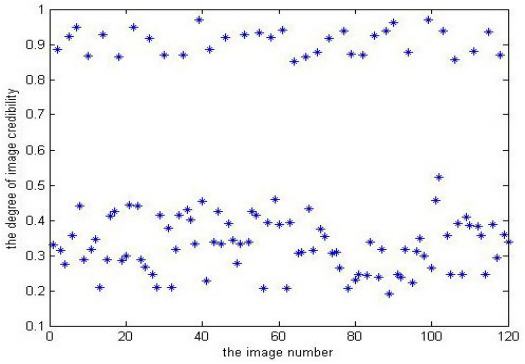
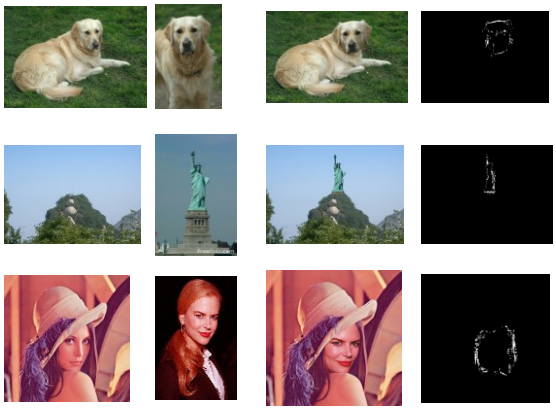


Fig.9. The degree of image credibility for the test images.



(a) (b) (c) (d)

Fig.10. One of the experiment results. (a) and (b) are two original images, (c) is an image forgery, and the feather operation is used around the dog head (Statue of Liberty, or Nicole Mary Kidman' face). (d) is the detecting result using our technique, and the traces of feather operation are marked by white points.

Several experiment results of successful detection are shown in Figure 10. Columns (a) and (b) are two original images. Shown in column (c) is an image forgery by copying part of image (b) and pasting to (a), and the artificial feather operation is used around the pasted region. We show the experimental result in column (d), and the traces of feather operation are marked by white points. From column (d) we can see that the pasted regions are marked by white points. The degree of image credibility is computed for the nine images by using our method, and they are 91.94%, 89.09%, and 92.51% (top to bottom in column (a)), 89.78%, 90.32% and 91.11% (top to bottom in column (b)), 45.90%, 42.43%, 50.31% (top to bottom in column (c)). We can see that the degree of image credibility of forgery image (column (c)) is much lower.

(3) Discussion

We resize the 120 images (resize factor 0.5, 1, 2), and perform the same experiment on the resized images to find the impact of resizing to our method. The accuracy rates are showed in Table 1, and it suggests that our method performs well even if the presence of resizing.

Although our proposed method produces encouraging results, more effort is still needed to improve the accuracy of our approach. It must be mentioned that the results obtained can be affected by the presence of other post-processing. We randomly selected some images from these tampered image open databases, such as the tampered database from Columbia University and Chinese Academy of Sciences. A successful example is showed in Fig.11, several failure examples in Fig.12. It is obvious that we can't detect these image tempered with post-processing or these without any processing spliced directly. In Fig.12, the right girl in the first origin image is feathered and moved from another image, and the hue adjustment is used for the whole forgery. The second origin image was made by splicing one image with mountain and other image with blue sky and white cloud. The third image was made by directly splicing two images without any post-processing. Our method fails to detect these tampered images, because the regularity brought by the feather operation is destroyed by other post-processing. Also, although with very little possibility, a few original images may be detected as a forgery one, if the image was taken in a specific scene or the edge of objects in the image was smooth extraordinarily. As shown in Fig.12, the edge of the left girl is original but originally smooth, and some segments of its edge are mistaken for the traces of feather operation, shown in region A. The second and the third origin images can't be detected because of no feather operation.

TABLE 1. THE ACCURACY OF DETECTING FEATURE OPERATION

feather radius	number	Accuracy(resize factor)		
		1	0.5	2
No feather	30	29	27	28
$0.2 \le r < 1$	30	27	26	28
$1 \le r < 10$	30	28	28	29
$10 \le r \le 20$	30	30	30	30

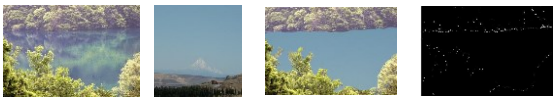
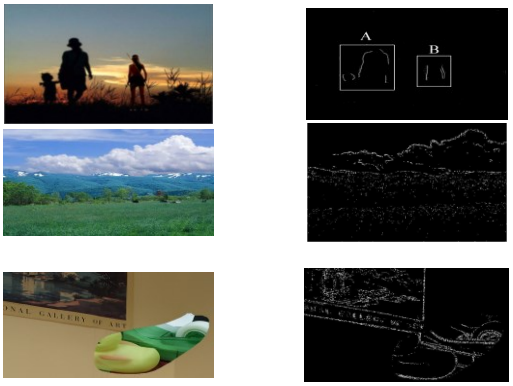


Fig.11. A successful example.



(a) image forgery (b) the failure result

Fig.12.Several failure examples.

In additional, the above-mentioned detecting feather operation to expose image forgeries was proposed in [15]. The local entropy of the gradient is used to determine the forged region in [15]. In this paper, we estimate each feather region pixel's gradient phase angle and feather radius, and the pixel's similarity to its neighbor pixels is defined to distinguish the feathered pixels from un-feathered pixels. Thought a lot of observations, we model feather operation. We don't need to train a classifier in advance. Compared with the method proposed in [15], our method is more effective.

VIII. CONCLUSION

Photo-shop has become the most attractive image-editing tool, and the feather operation has turned to be almost inevitable when tamping images. We propose a blind and efficient technique capable of exposing image forgeries by detecting the traces of feather operation. The degree of image credibility is defined to describe the reality of the image, which is more acceptable than just using a decision of YES or NO. The experimental results demonstrate that the proposed algorithm is reliable in discovering the traces of feather operation. However, when we don't use feather operation and other post-processing to tamper an image, the detection results will be unsatisfactory.

Considerable more work will be done hopefully in this area. We expect that the technique described in this paper will lead to the development of image forensics filed, and make it increasingly harder to create convincing image forgeries.

IX. ACKNOWLEDGMENTS

This work is supported by the National High Technology Research and Development Program("863" Program) of China (No. 2012AA011803) .

REFERENCES

[1] V.M.Potdar, S.Han, E.Chang,2005. survey of digital image watermarking techniques, IEEE International Conference on Industrial Informatics, pp.709-716.

[2] Tanzeela Qazi, 2013. Survey on blind image forgery detection, IET Image Processing, Volume 7, Issue 7, pp. 660-670.

[3] Yanping Huang, Wei Lu, Wei Sun and Dongyang Long, 2011. Improved DCT-based detection of copy-move forgery in images, Forensic Science International, Vol.206, pp.178–184.

[4] Jie Zhao, Jichang Guo, 2013. Passive forensics for copy-move image forgery using a method based on DCT and SVD, Forensic Science International, Vol 233, pp. 158–166.

[5] Weihai Li, Nenghai Yu, and Yuan Yuan, 2008. Doctored JPEG image detection, IEEE International Conference on Multimedia and Expo, pp.253-256.

[6] Qingzhong Liu, Peter A. Cooper, 2013. Detection of JPEG double compression and identification of smartphone image source and post-capture manipulation, Springer-Applied IntelligenceVol 39, pp.705‑726.

[7] Qu ZhenHua, Luo WeiQi, Huang JiWu, 2014. A framework for identifying shifted double JPEG compression artifacts with application to non-intrusive digital image forensics, Science China Information Sciences, vol.57, pp.028103:1-028103:18.

[8] H. Farid. 2009.Exposing digital forgeries from JPEG ghosts, *IEEE Transactions on Information Forensics and Security*, vol.4, no.1, pp.154-160.

[9] Hieu CuongNguyen,Stefan Katzenbeisser,2012.Performance and Robustness Analysis for Some Re-sampling Detection Techniques in Digital Images,Springer-Verlag Berlin Heidelberg, pp.387-397.

[10] Gajanan K. Birajdar,Vijay H. Mankarr,2014. Blind method for rescaling detection and rescale factor estimation in digital images using periodic properties of interpolation, Elsevier GmbH.

[11] Yongzhen Ke, Fan Qin, Weidong Min, Guiling Zhang, 2014.Exposing Image Forgery by Detecting Consistency of Shadow,The Scientific World Journal,Vol 2014.

[12] M.K.Johnson and H.Farid,2008. Detecting photographic composites of people, *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, vol.5041, pp.19-33.

[13] Y.Sutcu, B.Coskun, H.T.Sencar, and N.Memon,2007. Tamper detection based on regularity of wavelet transform coefficients, *IEEE International Conference on Image Processing*, vol.1, pp.397-400.

[14] Makkena Purnachandra Rao ect, 2014. Harnessing Motion Blur to Unveil Splicing, IEEE Transactions on Information Forensics and Security, vol. 9, pp.583-595.

[15] Zhe Li and Jiangbin Zheng, 2009.Blind detection of digital forgery image based on the local entropy of the gradient, *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, vol.5450, pp.161-169.

[16] Jiangbin Zheng and Miao Liu, 2009.A digital forgery image detection algorithm based on wavelet homomorphic filtering, *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, vol.5450, pp.152-160.

[17] Chang-Hee Choi, Hae-Yeoun Lee, Heung-Kyu Lee, 2013. Estimation of color modification in digital images by CFA pattern change, Forensic Science International, vol 226, pp. 94-105.

[18] A.Swaminathan, M.Wu, and K.J.R. Liu, 2008.Digital image forensics via intrinsic fingerprints, *IEEE Transactions on Information Forensics and Security*, vol.3, no.1, pp.101-117.

[19] A.Swaminathan, M.Wu and K.J.R.Liu,2007. Non-intrusive component forensics of visual sensors using output images, *IEEE Transactions on Information Forensics and Security*, vol.2, no.1, pp.91-106.

[20] M.Chen, J.Fridrich, J.Lukáš and M.Goljan, 2007.Imaging sensor noise as digital x-ray for revealing forgeries, *In Proc. 9th International Workshop on Information Hiding*, Saint Malo, France, *Lecture Notes in Computer Science*, vol.4567, pp.342-358.

[21] H. Gou, A.Swaminathan, and M.Wu, 2007. Noise feathers for image tampering detection and steganalysis, *in Proc. IEEE International Conference on Image Processing*, San Antonio, vol.6, pp.97-100.

[22] M.K. Johnson and H. Farid, 2006. Exposing digital forgeries through chromatic aberration, *in Proc. ACM Workshop on Multimedia and Security*, Geneva, Switzerland, pp.48-55.

[23] Y.F.Hsu and S.F.Chang,2007. Image splicing detection using camera response function consistency and automatic segmentation. *In Proc. IEEE International Conference on Multimedia and Expo*, Beijing, China, pp.28-31.

[24] Yu-Feng Hsu,2010. *Camera Response Functions for Image Forensics:*An Automatic Algorithm for Splicing Detection *Information Forensics and Security,*IEEE transaction on Signal Processing Society vol5, pp.816-825.

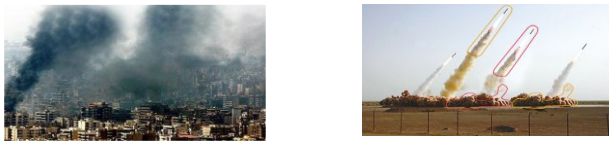
[25] Wei Lu, Wei Sun,Fu-Lai Chung,Hongtao Lu, 2011. Revealing digital fakery using multiresolution decomposition and higher order statistics,Engineering Applications of Artificial Intelligence,vol 24,pp. 666‑672.

[26] S.Bayram, I.Avcibas, B.Sankur and N.Memon,2006. Image manipulation detection, *J. Electron. Imaging*, vol.15, no.4, pp.41102.

[27] S.Bayram, İ.Avcıbaş, B.Sankur, and N.Memon, 2005. Image manipulation detection with binary similarity measures, *In Proc. European Signal Processing Conf*., Turkey.

[28] S.Di Zenzo,1986. A note on the Gradient of a Multi-Image, *Computer Vision*, Graphics and Image Processing, vol.33, pp.116-125.

Figure 1



(a) (b)

Fig.1.Examples of image forgeries obtained from internet (a) the published Reuters photograph showing the remnants of an Israeli bombing. (b) the published photograph showing four Iranian missiles streaking skyward.

Figure 2

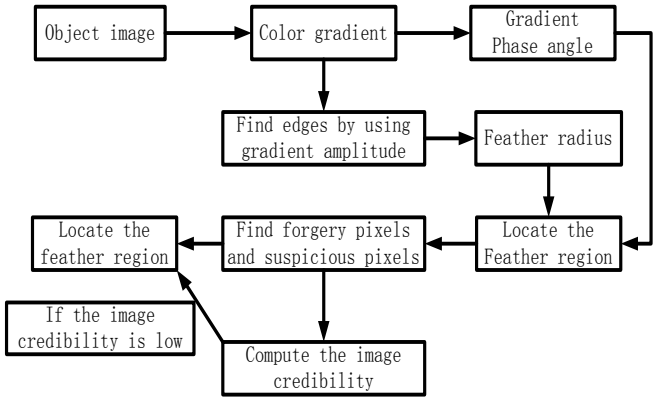
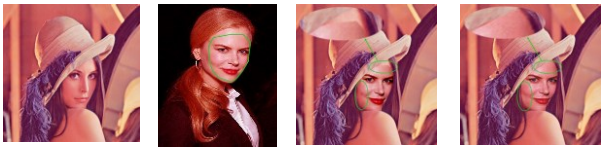


Fig.2 The flow chart of exposing image forgeries by detecting traces of feather operation

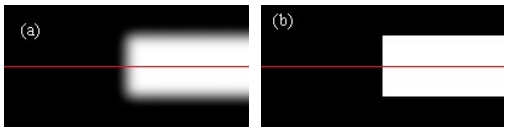
Figure 3



(a) (b) (c) (d)

Fig.3. Example for the most common image manipulations to create an image forgery. (a) is the original Lena image, (b) is the photo of Nicole Mary Kidman. (c) is a composite image forgery by copying Nicole Mary Kidman's face to Lena image. (d) is another composite image forgery, in which the traces of splicing around the face are not clear due to the feather operation.

Figure 4



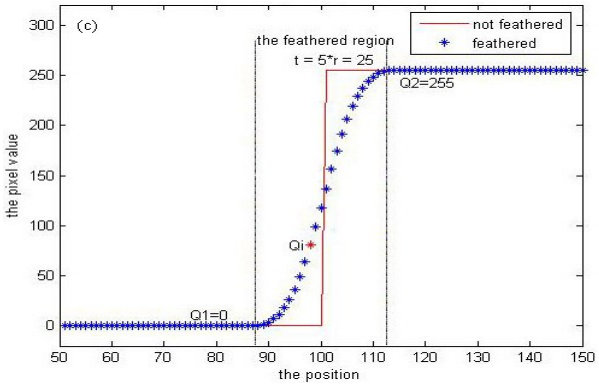


Fig.4. Feathered image (a) and un-feathered edge (b). Profile of the red line in (c) to show the difference between the feathered edge and un-feathered edge.

Figure 5

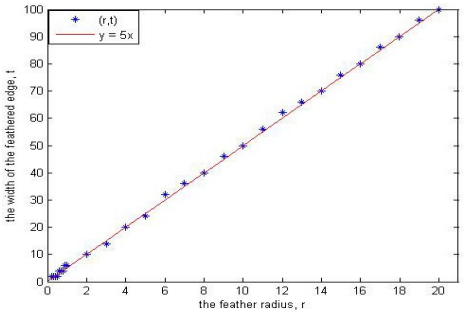


Fig.5. The relationship between t and r.

Figure 6

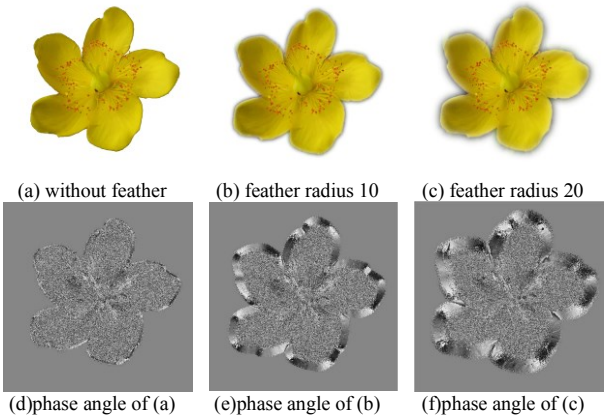


Fig.6. The influence of feather operation on the phase angle. Shown in the first row from left to right are the original image (a), the forgeries with feather radius $r = 10$ (b) and $r = 20$ (c). Shown in the second row are the gradient phase angle images respectively.

Figure 7

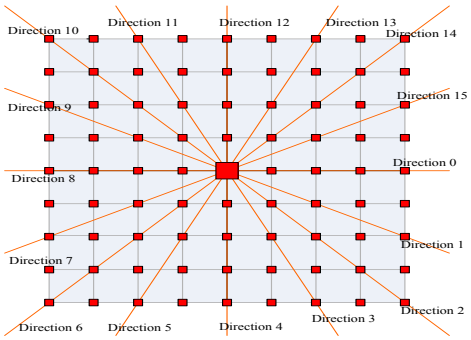


Fig.7. The 16 directions around the center pixel.

Figure 8

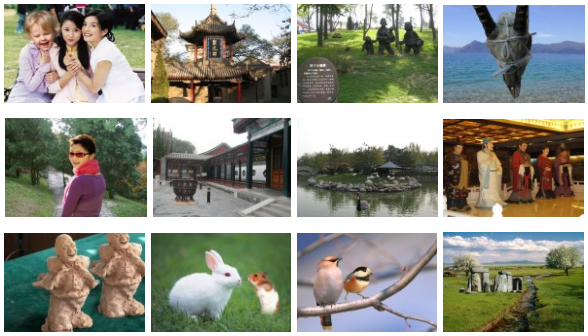


Fig.8. Some representative test images.

Figure 9

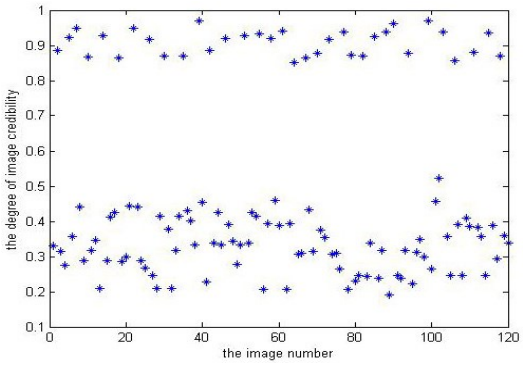
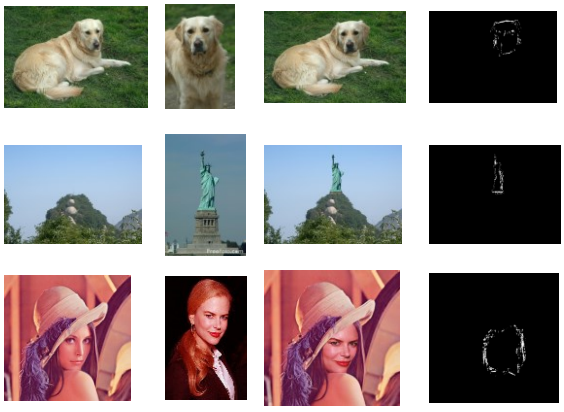


Fig.9. The degree of image credibility for the test images.

Figure 10



(a) (b) (c) (d)

Fig.10. One of the experiment results. (a) and (b) are two original images, (c) is an image forgery, and the feather operation is used around the dog head (Statue of Liberty, or Nicole Mary Kidman' face). (d) is the detecting result using our technique, and the traces of feather operation are marked by white points.

Table 1

TABLE 1. THE ACCURACY OF DETECTING FEATURE OPERATION

feather radius	number	Accuracy(resize factor)		
		1	0.5	2
No feather	30	29	27	28
$0.2 \le r < 1$	30	27	26	28
$1 \le r < 10$	30	28	28	29
$10 \le r \le 20$	30	30	30	30

Figure 11

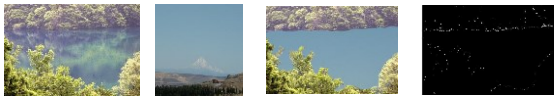
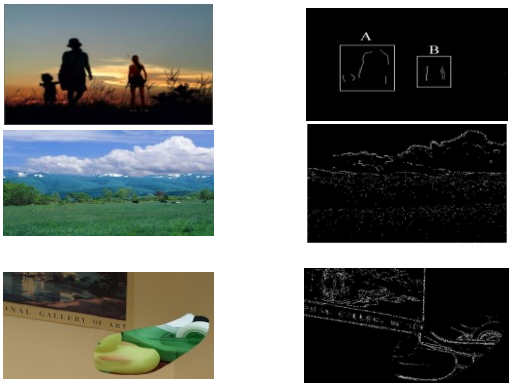


Fig.11. A successful example.

Figure 12



(a) image forgery (b) the failure result

Fig.12.Several failure examples.