Digital image forgery detection and estimation by exploring basic image manipulations

Article *in* Digital Investigation · February 2012

DOI: 10.1016/j.diin.2011.06.004

Digital Investigation 8 (2012) 215–225

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Digital image forgery detection and estimation by exploring basic image manipulations

S. Devi Mahalakshmi [a,*], K. Vijayalakshmi [b], S. Priyadharsini [a]

[a] *Computer Science and Engineering Department, Mepco Schlenk Engineering College, Mepco Engineering College (PO), Sivakasi 626005, Virudhunagar, Tamilnadu, India*

[b] *Information Technology Department, Mepco Schlenk Engineering College, Sivakasi 626005, India*

ARTICLE INFO

Article history:
Received 8 June 2011
Accepted 19 June 2011

Keywords:
Digital forensics
Digital image forgery
Fake image
Interpolation
Rescaling
Rotation
Contrast enhancement
Histogram equalization

ABSTRACT

In this modern age in which we are living, digital images play a vital role in many application areas. But at the same time the image retouching techniques has also increased which forms a serious threat to the security of digital images. To cope with this problem, the field of digital forensics and investigation has emerged and provided some trust in digital images. In this paper we proposed a technique for image authentication that detects the manipulations that are done in the digital images. In most of the image forgeries such as copy-and-paste forgery, region duplication forgery, image splicing forgery etc basic image operations or manipulations are often involved. Thus if there exists the evidence for basic image alterations in digital images we can say that the image has been altered. This paper aims at detecting the basic image operations such as re-sampling (rotation, rescaling), contrast enhancement and histogram equalization which are often done in forged images. The available interpolation related spectral signature method is used for detecting rotation and rescaling and for estimating parameters such as rotation angle and rescale factors. This rotation/rescaling detection method detects some unaltered images as altered one when the images are JPEG compressed. We have overcome that problem by adding noise in the input images. We have also used the existing fingerprint detection technique for detecting contrast enhancement and histogram equalization. Besides the techniques discussed in the existing method, we identified a unique property for histogram equalization which can help us to differentiate contrast enhancement from histogram equalization. This work is tested in USC-SIPI database which consists of general unaltered images and achieved results with satisfactory accuracy.

1. Introduction

Digital image forgery is the process of manipulating the original photographic images to create the forged image. Digital forensics aims to detect the alterations done in the images by investigating the images. With the usage of powerful image editing tools such as Paint, Photoshop etc, numerous image retouching techniques have become practical. Fake images are sometimes created for amusements and advertisements such as a cat playing guitar, baby smoking cigarette. These fake images used in harmless environments are not bad. But at the same time, malicious alteration of image content forms a serious threat to the security of digital images. Digital images used in law and order places should be genuine and so the image forgery detection techniques play a major role in these places.

The fake or forged images are created with the aim of altering the information present in the original images. In most of the forged images basic image operations such as rotation, rescaling, stretching, zooming, and enhancing

[*] Corresponding author. Tel.: +91 9942349553.
E-mail address: sdevi@mepcoeng.ac.in (S. Devi Mahalakshmi).

1742-2876/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2011.06.004

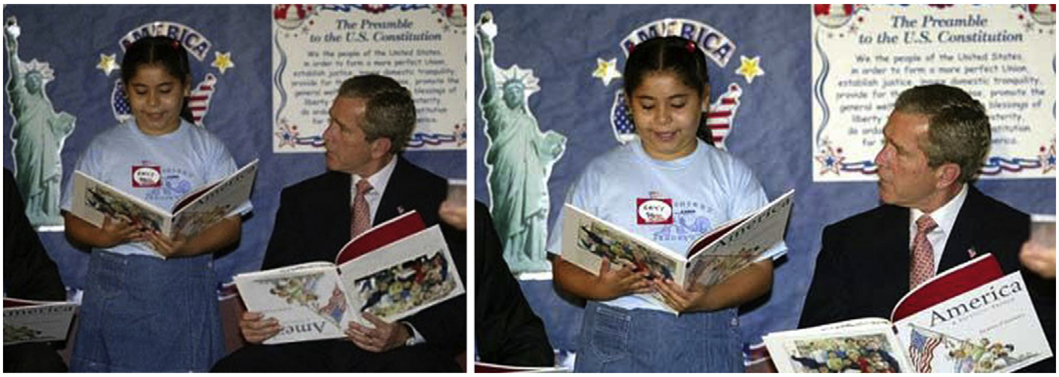

Fig. 1. The fake image (left) showing George Bush holding the book upside down at a school and its original one (right).

contrast are often involved. In many applications there is the need to detect whether the image has been retouched or not instead of detecting which type of forgery is involved. In such cases our detection method can be used as it detects the basic image alterations performed in the digital images. Consider a copy-and-paste forgery. In this forgery, an image region is copied from image and pasted either in the same or different image. To make the copied region fit in the original image and to make the forged image look natural the image manipulations are performed. Therefore detecting the image manipulations discussed in our proposed technique is still forensically significant.

Fig. 1 shows an example for fake image generated in real life and its original one. In 2002, this fake photograph was widely circulated to show President George Walker Bush holding a children's book upside down during a photo opportunity at a grade school. Seasoned photo experts, however, noticed that the photo on the back of the book Bush is holding is a left-to-right mirror image of the one that the girl is holding, and proved that it had been photo manipulated. Nonetheless, the picture was and continues to be cited as evidence of the former president's supposed lack of intelligence.

Fig. 2 shows another example for the fake image and its original one. In September 2010, Egypt's largest newspaper, the state-run Al-Ahram, showed a forged photo of world leaders walking the red carpet during Middle East peace talks at the White House. It was notable in that Egyptian President Hosni Mubarak is leading the way, ahead of even President Barack Obama in his own residence. It didn't take long for observers to figure out the Al-Ahram photo was an alteration. Not only the floor and the rest of the background are awkwardly cropped out, making it appears as if the leaders are walking on a flying carpet, and there are clearly visible borders around Mubarak where he'd been repositioned in front of Obama and Palestinian Authority President Mahmoud Abbas.

This paper is organized as follows: Section 2 describes about the existing works for image forgery detection and their limitations. Section 3 explains the methodology of our proposed system. Section 4 discusses about the results of the proposed system and also discusses the detection performance of the proposed system followed by conclusion and future work provided in Section 5.

2. Related works

In recent years, many image forgery detection techniques have been proposed and we have surveyed some of the existing methodologies for forgery detection here. The existing approaches can be classified into two categories: Active or Non-blind approach and Passive or Blind approach.

Active forgery detection techniques require prior knowledge about the original image such as a reference template, or features extracted from the original. Therefore they are not automatic. These methods have limited values in applications since the original image is unavailable in

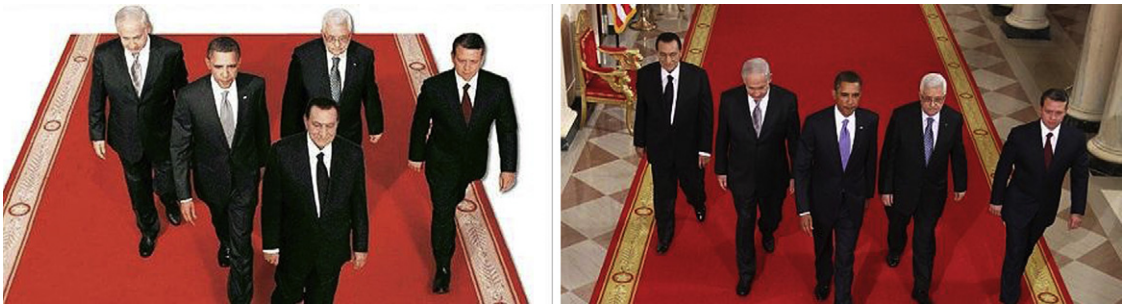

Fig. 2. The fake image (left) of World Leaders in the White House and its original one (right).

most practical cases. Digital Watermarking (Cox et al., 2002; Liu et al., 2008) is a popular active detection technique for authenticating images. It works by inserting an imperceptible digital code (a watermark) into the image at the time of recording. With the assumption that tampering will alter a watermark, an image can be authenticated by verifying that the extracted watermark is the same as that which was inserted. The major drawback of watermarking scheme is that a watermark must be inserted at precisely the time of recording, which would limit this approach to specially equipped digital cameras. Some earlier methods for detecting rotation and estimating rotation angle have been reported. In Greenspan et al. (1994), rotation angle estimation was carried out from texture features using a steerable oriented pyramid which was used to extract features for the input textures, followed by a supervised classification. Onishi and Suzuki (1996) used a modified version of Hough transform to the reference and input images, and uniquely computed the angle of rotation. A rotation invariant template matching method based on the combination of a projection method and Zernike moments was proposed to estimate rotation angle in Choi and Kim (2002). In Xiong and Quek (2006), the rotation angle between the input and the reference images was obtained from the peak of angle histogram generated through a voting procedure. Ulas et al. (2007) studied rotation angle estimation of textures aiming at a real-time implementation. Though these methods yielded good results, they are active methods and hence can't be used in real time applications.

Passive methods are the newly developed techniques and have wider usage since they require nothing from the image taker. As given in (Farid, 2009) the passive detection techniques can be roughly grouped into five categories: (1) Pixel-based (Fridrich et al., 2003; Popescu and Farid, Feb. 2005) (2) Format-based (Farid, 2008; Lukas and Fridrich, 2003) (3) Camera-based (Johnson and Farid, 2006a; Popescu and Farid, 2005) (4) Physics-based (Johnson and Farid, 2005; Johnson and Farid, 2007a) and (5) Geometric-based (Johnson and Farid, 2007b; Johnson and Farid, 2006b) techniques. H. Farid provided a survey on all these categories in Farid (2009) and explained the forensic methods within each of these categories.

Several passive techniques for image authentication based on detecting image operations have been already reported. Popescu and Farid (Feb. 2005) presented a method to find the rescaling traces hidden in any portion of an image without resorting to a reference image by using expectation maximization (EM) (Dempster et al., 1977). Mahdian and Saic (2008) used periodicity due to interpolation to perform blind image authentication. They introduced Radon transform on the basis of second derivative to detect rotation without estimation of the rotation angle. Gallagher (2005) proposed a rescaling detection method. This method exploits periodicity in the interpolated image for detecting the traces of rescaling. Motivated by Gallagher method Wei et al. (2010) developed a unified way to determine parameters of rescaling and rotation. But Gallagher (2005) and Wei et al. (2010) detects only rotation and rescaling operations done in the forged images. This is not sufficient and so we proposed methods to detect rotation, rescaling, contrast enhancement and histogram equalization. Stamn and Liu (2010) proposed a technique for detecting the pixel value mapping operations such as contrast enhancement. According to Stamn and Liu (2010), the pixel value mapping operations leave behind some statistical traces called as intrinsic fingerprints in the image's pixel value histogram. By detecting the intrinsic fingerprints the pixel value mapping operations done in the image can be identified. The limitation in this work is that it

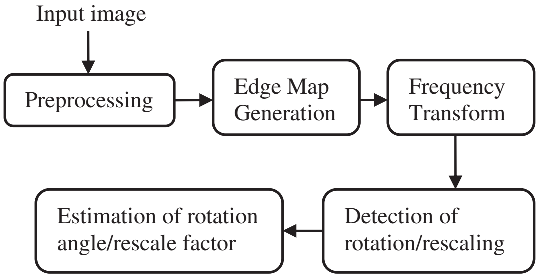
Input image
Preprocessing
Edge Map Generation
Frequency Transform
Detection of rotation/rescaling
Estimation of rotation angle/rescale factor

Fig. 3. The steps in re-sampling detection method.

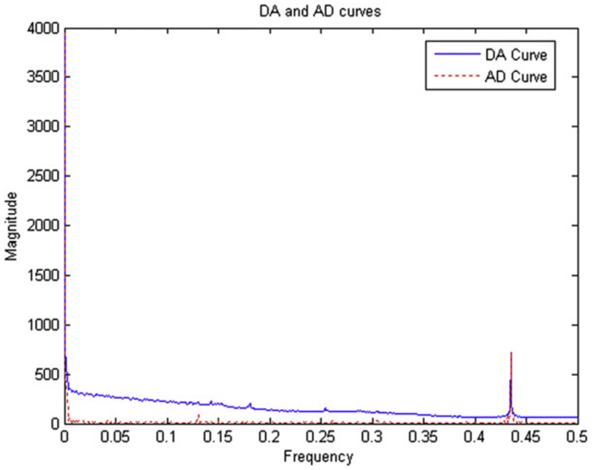

Fig. 4. The DA and AD curves of rescaled Baboon image.

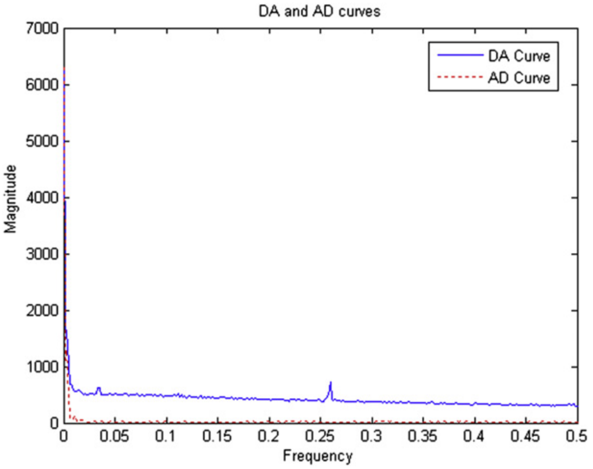

Fig. 5. The DA and AD curves of rotated Baboon image.

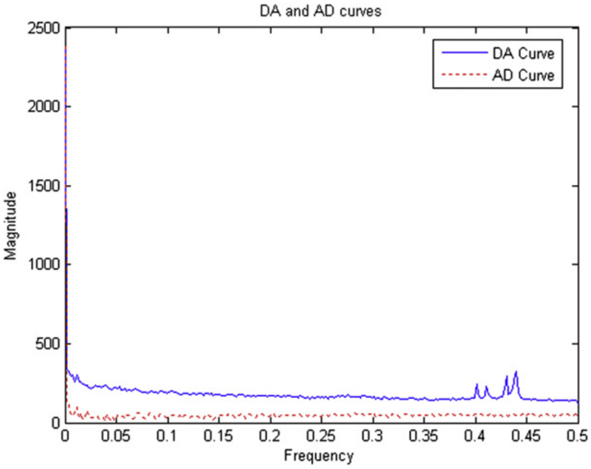

Fig. 6. The DA and the AD curves of unaltered, JPEG compressed Peppers image before noise addition.

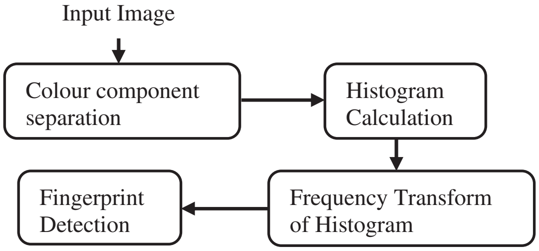

Fig. 8. The steps in contrast enhancement detection method.

doesn't detect rotation/rescaling and hence it won't detect all the forged images. Our method combines the techniques in Gallagher (2005), Wei et al. (2010), Stamn and Liu (2010) and detects the operations such as rotation, rescaling, contrast enhancement and histogram equalization. As these four operations are involved in most of the forged images our proposed work detects almost all the forged images.

The motivation of our work can be summarized as follows: The active image forgery detection techniques detect the forgeries that are present in the digital images using prior knowledge about the original image. But in real time applications the original image is not available. Some passive detection techniques like Pan and Lyu (2010) are limited to detect specific types of image forgery. These methods also fail to detect forged images if the image has undergone other types of forgery. Therefore detecting the manipulations involved in the digital images is the dominant way to detect the forged images. Though there are methods like Gallagher (2005), Wei et al. (2010), Stamn and Liu (2010) for detecting the image manipulations, they are limited to detecting either one or two image operations. All these have become motivation for the development of our work which is the improved forensic technique.

3. Proposed work

In this paper, the method for detecting image alterations such as re-sampling, contrast enhancement and histogram equalization has been proposed. This method also estimates the parameters of the rotation and rescaling operation. In the forged images, the image alterations may be performed either to the entire image (global) or to the specified portions (local) of the image. Our work detects both global and local image alterations. As mentioned earlier, we used the rescaling detection algorithm described in Gallagher (2005) and rotation detection algorithm described in Wei et al. (2010) and contrast enhancement/histogram equalization described in Stamn and Liu (2010). By combining all these techniques we achieved a combined method for detecting rotation, rescaling, contrast enhancement and histogram equalization. We also improved the performance of algorithm specified in Gallagher (2005) and Wei et al. (2010).

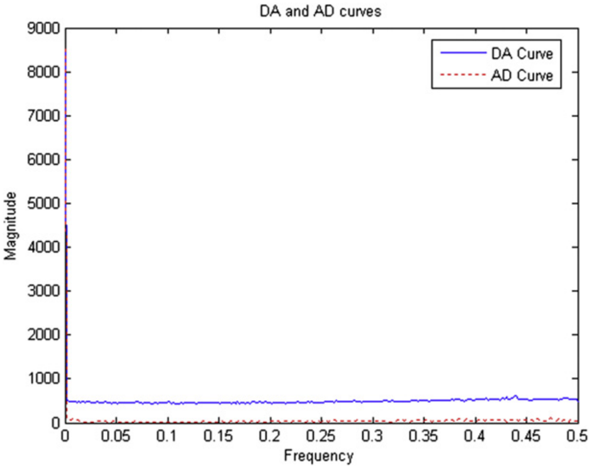

Fig. 7. The DA and the AD curves of unaltered, JPEG compressed Peppers image after noise addition.

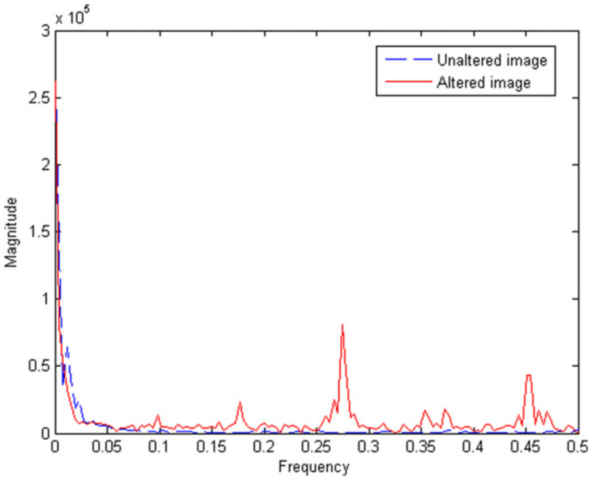

Fig. 9. The frequency plots of an image before and after contrast enhancement.

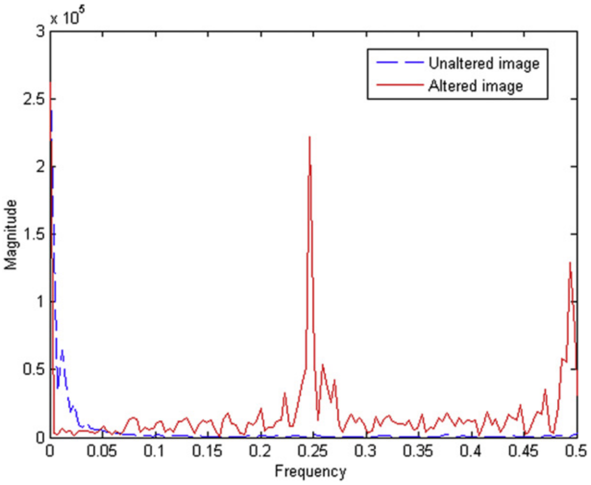

Fig. 10. The frequency plots of an image before and after histogram equalization.

3.1. *Re-sampling detection method*

We used the method described in Gallagher (2005) and Wei et al. (2010) for detecting re-sampling in digital images. The steps in the method for detecting re-sampling are given in Fig. 3. As shown in the Fig. 3, the detection technique consists of five steps: (1) Pre-processing (2) Edge map generation (3) Frequency transformation (4) Detection of rotation/rescaling (5) Estimation of rotation angle/ rescaling factor.

3.1.1. *Pre-processing*

The input image is first converted into the YCbCr color space. The motivation for choosing YCbCr color space is that it is perceptually uniform and is a better approximation of the color image processing. The luminance component that is the Y component alone is then separated from the YCbCr color image.

3.1.2. *Edge map generation*

A pattern of second order difference, i.e., the edge map of the input image is generated by convolving the luminance (Y) component of the input image with 3 × 3 Laplacian operator. Thus the remaining steps are done on the edge map of the input image.

3.1.3. *Frequency transformation*

The one dimensional DFT is calculated for the edge map. There are two methods for calculating the DFT such as DA (DFT + Averaging) and AD (Averaging + DFT) methods.

In DA Method, the magnitude of DFT is calculated for each row of the edge map and then the average is taken over all the rows to get the horizontal spectrum. Assume that$E(m,n), m\in[1,M],\ \ n\in[1,N]$ are the entries of the edge map and F is the Discrete Fourier Transform. The DA method can be expressed as follows:

$$E_{DA} = \frac{1}{M}\sum_{m-1}^{M}|F[E(m,n)]| \tag{1}$$

In AD Method, the average of all rows of the edge map is calculated to form a horizontal row and then the magnitude of DFT is calculated to get the horizontal frequency spectrum. The AD method can be defined as follows:

$$E_{AD} = \left|F\left[\frac{1}{M}\sum_{m-1}^{M}E(m,n)\right]\right| \tag{2}$$

3.1.4. *Detection of rotation/rescaling*

The horizontal frequency spectra obtained from DA and AD methods are plotted separately against frequencies to form DA and AD curves respectively. Only half of the curve is considered because the DFA plot is symmetrical. Peaks appear in DA and AD curves because of maximum magnitude value in the frequency spectrum if the image is resampled. The appearance of peaks is due to interpolation. When an image or image block is re-sampled, interpolation takes place in the re-sampled image or image block. The interpolated regions and their derivatives have inherent periodicity. Due to interpolation-induced periodicity, the frequency spectrum contains peaks directly related to the scaling factors (Remember in rotation also the image is rescaled with a scaling factor proportional to rotated angle). The frequencies of the peaks formed referred as peak frequency are used for estimating the rotation angle and rescale factor.

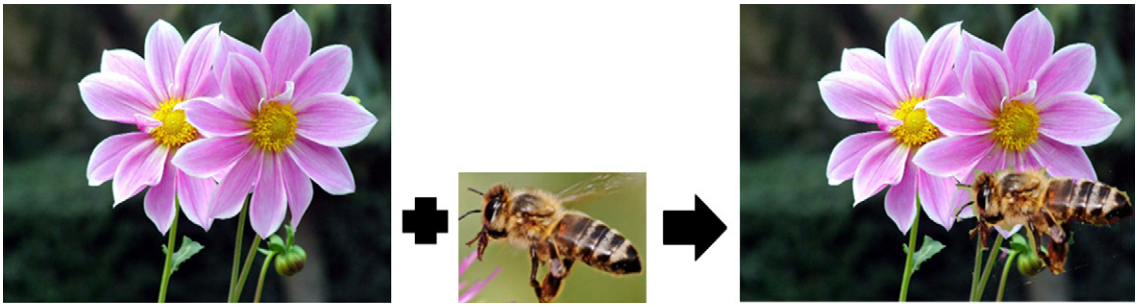

Fig. 11. The original flower and bee images (first and second) and the forged image (third) obtained by rotating the bee image by 15° and pasting it to the flower image.

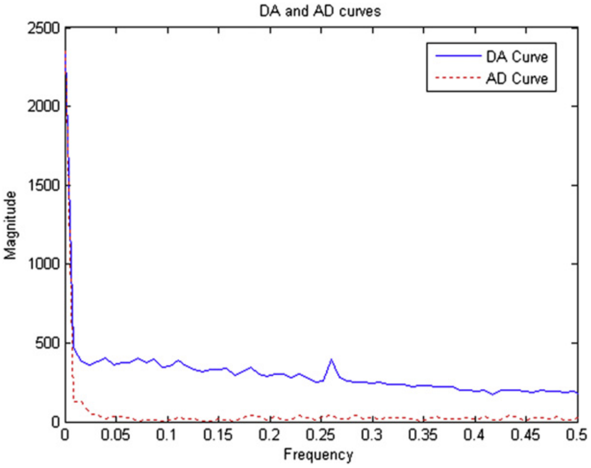

Fig. 12. The DA and AD curves of one of the fake image blocks of the forged image. A peak appears at 0.26 in DA method because of rotation by 15°.

The reason for using two methods (DA and AD) is for distinguishing rotation and rescaling. Though rotation and rescaling behaves in a similar manner, they differ in certain cases which may be used for distinguishing them. Peaks formed due to rotation appear only in DA method and the peaks formed because of rescaling appear in both DA and AD methods.

3.1.5. *Estimation of rotated angle/rescale factor*

The rotated angle/rescale factor can be estimated by using the peak frequency obtained from the DA and AD curves. Rotation angle estimation formula is given as follows:

$$f_{rot1} = \begin{cases} 1 - \cos\Theta, & 0^\circ < \Theta \le 60^\circ \\ \cos\Theta, & 60^\circ < \Theta < 90^\circ \end{cases} \tag{3}$$

and

$$f_{rot2} = \begin{cases} \sin\Theta, & 0^\circ < \Theta \le 30^\circ \\ 1 - \sin\Theta, & 30^\circ < \Theta < 90^\circ \end{cases} \tag{4}$$

where Θ is the rotated angle and f_{rot1}, f_{rot2} are the peak frequencies induced due to rotation. The rescale factor estimation formula is given as follows:

$$f_{res} = \begin{cases} 1 - 1/R, & 1 < R \le 2 \\ 1/R, & R > 2 \end{cases} \tag{5}$$

or

$$f_{res} = 1/R - 1, \quad R < 1 \tag{6}$$

where R is the rescale factor and f_{res} is the peak frequency induced due to rescaling. The first equation is used when the image size is enlarged and the second equation is used when the image size is reduced. By substituting the obtained peak frequency from DA and AD curve in the above estimation formulae, Θ or R can be calculated. The formation of rescale factor and rotation angle estimation formulae can be referred from Gallagher (2005) and Wei et al. (2010).

Let us see one example for rescaling detection algorithm. Assume that the Baboon image is rescaled by a factor of $R = 2.3$. Image enlargement has been performed and the condition $R > 2$ is met. Therefore from Eq. (5), the peak should appear at $1/R = 1/2.3 = 0.43$. This peak should also be visible in both DA and AD curves. Fig. 4 shows the DA and AD method plots of the rescaled image.

An example for rotation detection algorithm is considered by rotating the Baboon image by 15°. The peaks should appear only in DA curve at 0.26 and 0.03. The DA and AD curves are shown in Fig. 5.

3.2. *Successive rotation and scaling detection*

In most of the forged images rotation and rescaling are involved in a combined manner. Different combinations of rotation and rescaling can also be distinguished and the parameters can be estimated using the re-sampling detection method. The four possibilities are double zooming (DZ), rotation-zooming (RZ), zooming-rotation (ZR), and double rotation (DR). In all these successive operations the peaks induced by first operation will not appear whereas the peaks due to second operation will appear. Also some peaks will appear at composite frequencies because of the combined operation. The combined operation peaks won't appear in AD curve if rotation is one of the operations.

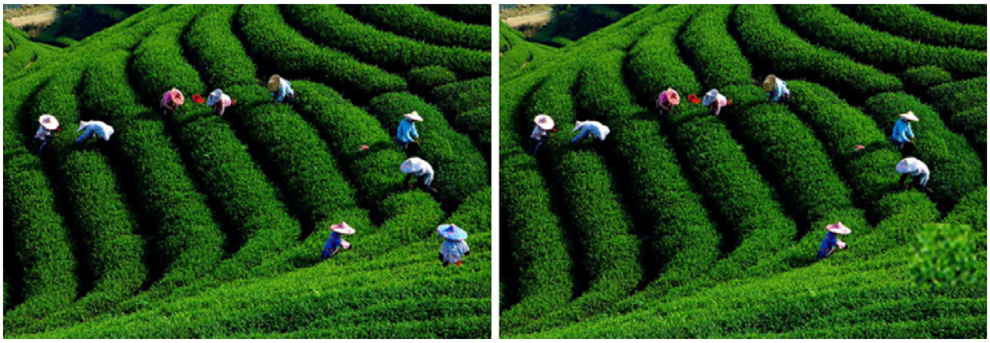

Fig. 13. The original image (left) and the forged image (right) obtained by copying and rescaling an original image block and pasting it within that image.

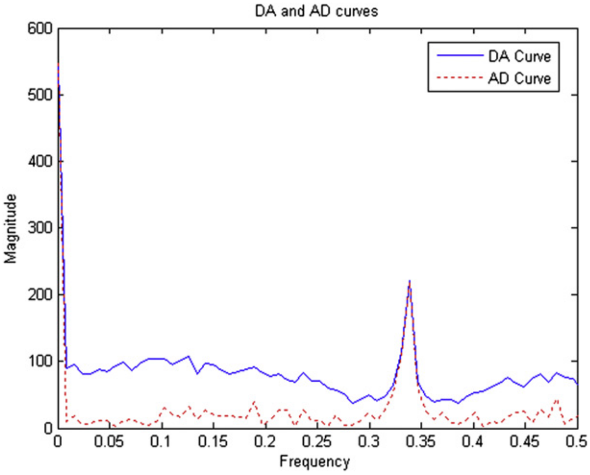

Fig. 14. The DA and the AD curves of one of fake image blocks of the forged image. A peak appears at 0.33 in both methods because of rescaling by a factor of 3.

3.2.1. *Double zooming detection*

Assume the image is double zoomed. Assume the first scaling factor is R_1 and the second zooming factor is R_2. The peaks due to R_1 won't appear. The spectral peaks are produced at $1/R_2$, $1 - 1/R_2$ or$1/R_2 - 1$ and as a result of successive operations, at several composite frequencies that are multiplications of single zooming frequencies such as

$$f_{DZ} = 1/(R_1R_2) \quad \textit{and} \quad f_{DZ} = (1/R_1)(1 - 1/R_2) \tag{7}$$

3.2.2. *Rotation-zooming detection*

In image forgery using a copy-move method, the inserted object may be rotated and rescaled to merge into the surroundings. Assume that the rotation angle is Θ, corresponding to the peak frequencies at $\sin\Theta$, $\cos\Theta$, $1 - \sin\Theta$, and $1 - \cos\Theta$ that would have appeared without further geometric transformation. After rotation, if the image is rescaled with a factor R, it leads to peaks at $1/R$, $1 - 1/R$ and $1/R - 1$, and a number of composite frequencies such as

$$f_{RZ} = (1/R)\sin\Theta \quad \textit{and} \quad f_{RZ} = (1/R)(1 - \cos\Theta) \tag{8}$$

3.2.3. *Zooming-rotation detection*

Let the zooming factor be R, and the subsequent rotation angle Θ. The rotation introduces peaks at frequencies $\sin\Theta$, $\cos\Theta$, $1 - \sin\Theta$, and $1 - \cos\Theta$, and several composite frequencies such as

$$f_{ZR} = (1/R)\sin\Theta, \quad f_{ZR} = (1 - 1/R)\sin\Theta \quad \textit{and} \quad f_{ZR} = (1/R)\cos\Theta \tag{9}$$

3.2.4. *Double rotation detection*

Suppose the first rotation angle is Θ_1 corresponding to peaks at frequencies $\sin\Theta_1$, $\cos\Theta_1$, $1 - \sin\Theta_1$, and $1 - \cos\Theta_1$ that would have appeared if no further operations were performed. The second rotation causes peaks at $\sin\Theta_2$, $\cos\Theta_2$, $1 - \cos\Theta_2$ and $1 - \sin\Theta_2$, as well as composite frequencies such as

$$f_{DR} = \sin\Theta_1\cos\Theta_2 \quad \textit{and} \quad f_{DR} = \cos\Theta_1\sin\Theta_2 \tag{10}$$

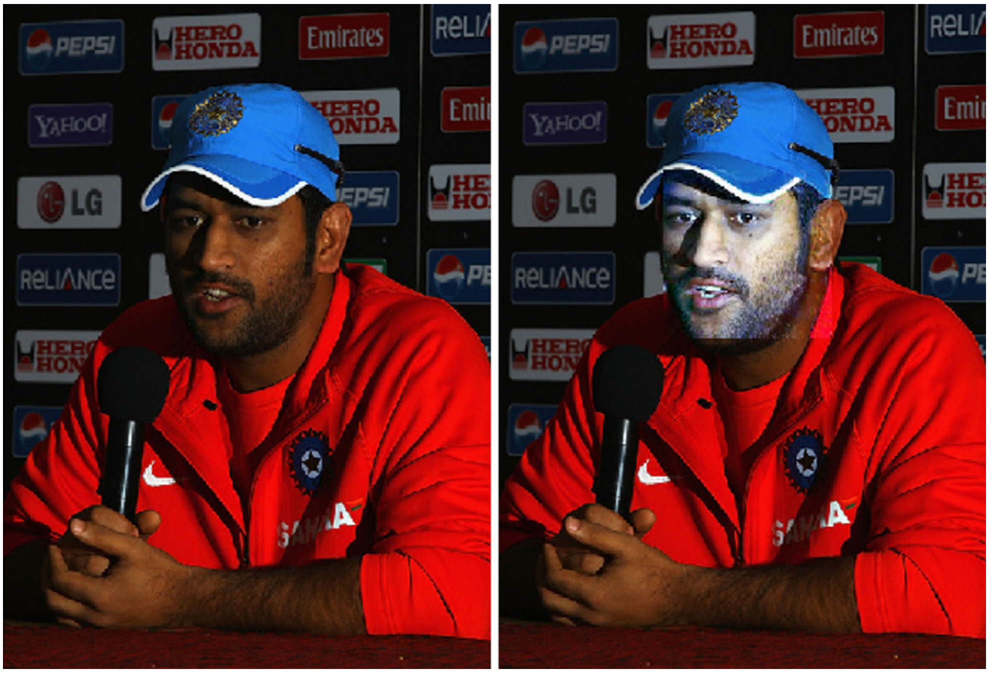

Fig. 15. The original image (left) and the forged image (right) obtained by local contrast enhancement.

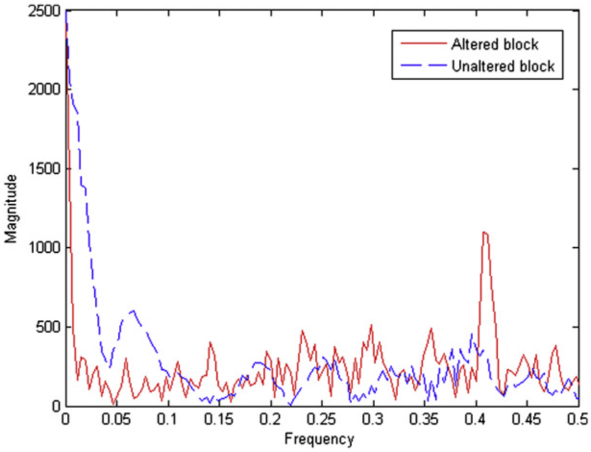

Fig. 16. The frequency spectrum plot of unaltered block and one of the altered blocks of the forged image. A striking peak appears in the plot of altered image block.

Wei et al. (2010) have given detailed explanation about the re-sampling detection and the successive rotation and scaling detection using separate examples. The local re-sampling is detected in the images by dividing the test image into overlapping blocks of size $B \times B$ having the overlapping area $L \times B$ where $L < B$. For each individual block the re-sampling detection algorithm is applied. If peak values exist in the average frequency spectrum of any block, the corresponding peak frequency is noted and the parameters are estimated from parameter estimation formulae. The blocks in which peaks exist are said to be suspicious blocks.

3.3. Noise addition for JPEG compression attack

When a doctored photograph is created by digitally compositing individual images, it may be often required to re-sample the image to make it look natural. Most of the forged images are saved in JPEG format after doing editing work. The proposed re-sampling detection method indicates the presence of re-sampled image regions in an image. However this detection method is not exact because this method is susceptible to JPEG attacks. The reason is that the periodic JPEG blocking artifacts coincide with the periodic patterns introduced by re-sampling.

In this paper, we proposed a method to suppress the periodic artifacts introduced by JPEG while retaining the re-sampling induced periodicity. Thus a new approach to suppress JPEG artifacts by adding Gaussian noise for robust detection of image resizing/rotation has been proposed. In forensics, suitable post-processing on the image can be performed without worrying about its visual quality, as the processed image is just meant for forensic analysis. Therefore adding Gaussian noise is an effective technique to mask the effects of JPEG. Controlled amounts of Gaussian noise are added to the resized/rotated and JPEG compressed image. By adjusting the noise level, the JPEG induced frequency components are suppressed while the interpolation-induced peaks are retained. Hence, the proposed method works even after JPEG compression.

Consider an unaltered Peppers image stored in JPEG format and compressed with maximum quality factor. As shown in Fig. 6, the DA method plot of the original image has some peaks. The DA and AD method plots of the original image after adding Gaussian noise of variance 0.01 is shown in Fig. 7. It is clear from the results that the peaks due to JPEG compression are suppressed thus proving that the Peppers image is unaltered.

3.4. Contrast enhancement detection

The method for detecting global and local contrast enhancement is also called as Intrinsic Fingerprint detection technique. The steps for detecting contrast enhanced images are shown in Fig. 8.

The test image may be a gray scale image or color image. If the image is RGB image, it is first separated into Red component, Green component and Blue component. The histogram of the image's pixel value is calculated for either Red or Green or Blue component. The magnitude of DFT of the calculated histogram then calculated. The obtained magnitude is then plotted against the frequency to obtain the frequency plot. Sudden zeros or striking peaks present in the frequency plot are referred to as intrinsic fingerprints. The intrinsic fingerprint if exists in the plot then the image is said to be altered by contrast enhancement.

The formation of peaks in the frequency plot of contrast enhanced image is due to some specified reason. As the images are contrast enhanced the pixel values are increased than the original one. The increased pixel values consume more power and hence have greater energy. In other words,

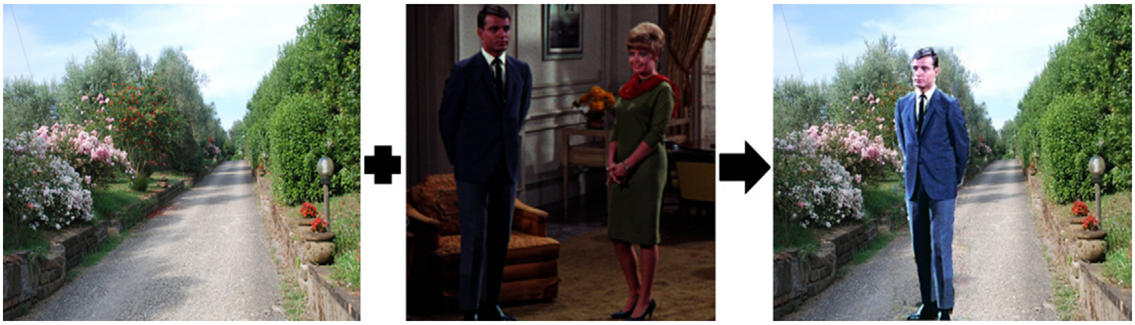

Fig. 17. The two original images (first and second) used for creating the forged image (third) which is an example for local histogram equalization.

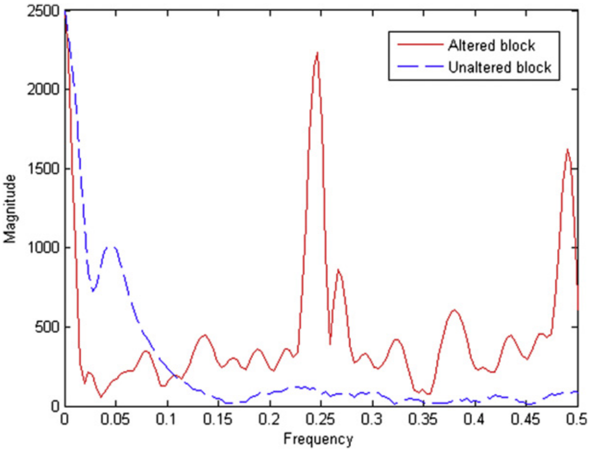

Fig. 18. The frequency spectrum plots of unaltered block and one of the altered blocks of the forged image. A striking peak appears in the plot of altered image block at 0.25.

an image requires more power to display white pixels than dark pixels. We are all aware of the energy saving search website Blackle.com powered by Google to remind us all of the need to take small steps in our everyday lives to save energy. Since energy is directly proportional to frequency, the enhanced images have high frequency components.

The local contrast enhancement is enhancing an image region within an image. This can be detected by dividing the image into nonoverlapping blocks of size $B \times B$ and repeating the above steps for each block.

Let us consider an example for contrast enhancement detection. The contrast of the original Peppers image is enhanced globally to create the altered image. The frequency plots of histogram of red layer of the original and the altered images are shown in Fig. 9. A striking peak exists in the curve of the enhanced image proving that the image is contrast enhanced. The original image is not available to the user. The result of forged image is compared with the original image just for to understand the concept clearly. In real time applications, the existence of striking peaks proves that the image has been altered.

3.5. Histogram equalization detection

The histogram equalization detection algorithm specified in Stamn and Liu (2010) uses a different technique other than the intrinsic fingerprint detection technique. As histogram equalization is also a form of contrast enhancement, the histogram equalized image will also have increased pixel values resulting in the increased energy. Therefore we used the same intrinsic fingerprint detection method for detecting histogram equalized images. While applying the intrinsic fingerprint detection technique to histogram equalized images, we analyzed a unique property for histogram equalized images. All the histogram equalized images produce a sudden peak at the peak frequency 0.25. If the histogram equalization is done in the localized image regions, the corresponding block produced striking peak at 0.25.

Histogram equalization effectively increases the dynamic range of an image's pixel values by subjecting them to a mapping such that the distribution of output pixel values is approximately uniform. The mapping used to accomplish this is dependent upon the histogram of the unaltered image and is generated according to the following equation.

$$m_{he}(l) = round\left(255\sum_{t=0}^{l}\frac{h(t)}{N}\right) \tag{11}$$

where N is the total number of pixels in the image and $h(t)$ is the histogram value for pixel value t. Since a predefined mapping is used for all histogram equalized images, the occurrence of peak is also fixed for all images. Thus histogram equalization has a unique property which can be used for its detection and also for distinguishing contrast enhancement and histogram equalization.

The unique property of histogram equalization is shown in Fig. 10. The example Peppers image is histogram equalized globally and the frequency spectrum plot of unaltered and altered images are shown in Fig. 10.

4. Results and discussion

We have discussed the results of the proposed system in this section.

4.1. Re-sampling detection

Fig. 11 shows a forged image created from more than one images. As shown in Fig. 11, the original bee image is rotated by 15° and pasted into the original flower image to form the fake image after some post-processing. Block wise detection is performed. The frequency plots of one of the fake blocks obtained using DA and AD methods are shown in Fig. 12. From these plots, it is clear that there exists a peak at the frequency 0.26 in DA method alone. Therefore only rotation has been performed. When this peak frequency is substituted in the rotation angle estimator formula, the rotation angle is estimated to be 15°.

Fig. 13 shows an example for copy-paste forgery in which local rescaling is involved. In this example, an image block taken from the original image is rescaled by a factor

Table 1
Performance of various global forgery detection methods.

Type of Forgery	Global rotation	Global rescaling	Global contrast enhancement	Global histogram equalization
No. of forged images taken	300	300	300	300
Correctly detected forged images	295	297	300	300
Undetected forged images	5	3	0	0
Detection rate (%)	98.3	99	100	100

Table 2
Performance of various local forgery detection methods.

Type of Forgery	Local rotation	Local rescaling	Local contrast enhancement	Local histogram equalization
No. of forged images taken	300	300	300	300
Correctly detected forged images	289	293	295	298
Undetected forged images	11	7	5	2
Detection rate (%)	96.3	97.6	98.3	99.3

of 3 and again pasted into the original image with a purpose to hide one of the persons present in the original image. Block wise detection is done to identify fake blocks. Fig. 14 shows the frequency plots of one of the fake block obtained using DA and AD methods. The peak appears in both the methods at 0.333 showing that the forgery done is rescaling. The rescale factor is estimated as 3 by substituting the peak frequency in rescale factor estimator formula.

4.2. Contrast enhancement detection

Fig. 15 shows a locally contrast enhanced image. The altered image is obtained by enhancing the contrast of an image region from the original image and pasting the enhanced region in the same location in the original image. The results are shown in Fig. 16 with detected peaks.

4.3. Histogram equalization detection

The forged image in which local histogram equalization is done is shown in Fig. 17. The two original images shown in Fig. 17 were used to form the fake image. The man in the second original image is cropped and placed in the first original image. To match the lighting environment of foreign pixels in original image, the man cropped is histogram equalized. The results of the detection are shown in Fig. 18.

4.4. Performance evaluation

The proposed method is tested in images from USC-SIPI database. This database consists of many unaltered general images. These images are altered manually using Adobe Photoshop for testing the detection of alterations in the images. The testing is done in 300 altered images and the results of various global and local detection techniques are compared as shown in Table 1 and Table 2. Note that the test images taken in Tables 1 and 2 were not JPEG compressed. For all the JPEG compressed images our technique suppresses the peaks due to compression and retains the peaks due to interpolation after noise addition.

The performance of the detection technique is decreased in local detection techniques as the forgery is applied in very small area. The performance of local detection methods for rotation, rescaling, contrast enhancement and histogram equalization is given in Table 2.

5. Conclusion and future work

An image re-sampling detector and rotation angle/rescale factor estimator based on interpolation artifacts has been developed with satisfactory accuracy. Combined with this capability of locating rotated/rescaled small image patches has also been developed. The method can also be used to discover the image's successive rescaling and rotation operations. Since no time-consuming iteration is involved and the major operation performed in the detection is FFT, computation complexity of the algorithm is not high. The resampling detection algorithms fail when JPEG compression is performed. It has been shown that adding Gaussian noise is as an effective technique to mask the effects of JPEG.

A set of image forensic techniques capable of detecting global and local contrast enhancement and histogram equalization has also been proposed. In each of these techniques, detection depends upon the presence or absence of an intrinsic fingerprint introduced into an image's histogram by a pixel value mapping. The usefulness of local alteration (rotation, rescaling, contrast enhancement, histogram equalization) detection for different types of forgeries like cut and paste forgery is demonstrated.

Blind detection of image forgery is a difficult task. For the copy-move type of image tampering, reliable detection of very small image areas is still a challenge. When post-processing is done such as JPEG coding with a low quality factor, detection of image alterations becomes more difficult. Moreover, to evade rescaling/rotation detection, more sophisticated interpolation methods can be used, and image manipulations may be done to make the rescaling traces undetectable.

The image can also be forged without using the basic operations such rotation, rescaling, contrast enhancement and histogram equalization. All these have become motivations for the development of further improved forensic techniques. In recent years manipulating the video content to create video forgery is also becoming prevalent. Therefore forgery detection techniques should be further extended to videos.

References

Choi M, Kim W. A novel two stage template matching method for rotation and illumination invariance. Pattern Recognit 2002;35(1):119–29.

Cox IJ, Miller ML, Bloom JA. Digital watermarking. San Mateo, CA: Morgan Kaufmann; 2002.

Dempster AP, Laird NM, Rubin DB. Maximum likelihood from incomplete data via the EM algorithm. J Roy Stat Soc B Stat Meth 1977;39(1):1–38.

Farid H. Digital ballistics from jpeg quantization: a follow-up study. Dept Comp Sci., Dartmouth College, Tech. Rep. TR2008-638; 2008.

Farid H. Image forgery detection. IEEE Signal Process Mag Mar. 2009; 26(2):16–25.

Fridrich J, Soukal D, Lukás J. Detection of copy move forgery in digital images. In: Proc. Digital Forensic Research Workshop, Aug. 2003.

Gallagher AC. Detection of linear and cubic interpolation in JPEG compressed images. In: Proc. 2nd Canadian conf. computer and robot vision, Washington, DC; 2005. p. 65–72.

Greenspan H, Goodman S, Perona R. Rotation invariant texture recognition using a steerable pyramid. In: Proc. 12th IAPR Int. Conf Pattern Recognition, vol. 2; 1994. p. 162–167.

Johnson MK, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In: Proc. ACM multimedia and security workshop, New York, NY; 2005. p. 1–10.

Johnson MK, Farid H. Exposing digital forgeries through chromatic aberration. In: Proc. ACM Multimedia and security Workshop, Geneva, Switzerland; 2006a. p. 48–55.

Johnson MK, Farid H. Metric measurements on a plane from a single image. Dept Comput Sci, Dartmouth College, Tech. Rep. TR2006–579; 2006.

Johnson MK, Farid H. Detecting photographic composites of people. In: Proc. 6th Int. workshop on digital watermarking, Guangzhou, China; 2007a.

Johnson MK, Farid H. Exposing digital forgeries through specular highlights on the eye. In: Proc. 9th Int. workshop inf hiding, Saint Malo, France; 2007b. p. 311–325.

Liu H, Rao J, Yao X. Feature based watermarking scheme for image authentication. In: IEEE Int. conf. multimedia and expo; 2008. p. 229–232.

Lukas J, Fridrich J. Estimation of primary quantization matrix in double compressed JPEG images. In: Proc. digital forensic research workshop, Cleveland, OH; Aug. 2003.

Mahdian B, Saic S. Blind authentication using periodic properties of interpolation. IEEE Trans Inf Forensics Security Sep. 2008;3(3):529–38.

Onishi H, Suzuki H. Detection of rotation and parallel translation using Hough and Fourier transforms. In: Proc. IEEE Int. conf. image processing; 1996. p. 827–830.

Pan Xunyu, Lyu Siwei. Region duplication detection using image feature matching. IEEE Trans Inf Forensics Security Dec. 2010;5(4):857–67.

Popescu AC, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Trans Signal Process 2005;53(10):3948–59.

Popescu AC, Farid H. Exposing digital forgeries by detecting traces of resampling. IEEE Trans Signal Process Feb. 2005;53(2 Pt. 2):758–67.

Stamn MC, Liu KJ. Forensic detection of image manipulation using statistical fingerprints. IEEE Trans Inf Forensics Security Sep. 2010; 5(3):492–506.

Ulas C, Demir S, Toker O, Fidanboylu K. Rotation angle estimation algorithms for textures and their real time implementation on the FU-SmartCam. In: Proc. 5th Int. symp. image and signal processing and analysis; 2007. p. 469–475.

Wei W, Wang S, Tang Z. Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery. IEEE Trans Inf Forensics Security Sep. 2010;5(3):507–17.

Xiong Y, Quek F. Automatic aerial image registration without correspondence. In: Proc. 4th IEEE Int. conf. computer vision systems; 2006. p. 25–33.