Chapter 15

ENHANCING IMAGE FORGERY DETECTION USING 2-D CROSS PRODUCTS

Songpon Teerakanok and Tetsutaro Uehara

Abstract The availability of sophisticated, easy-to-use image editing tools means that the authenticity of digital images can no longer be guaranteed. This chapter proposes a new method for enhancing image forgery detection by combining two detection techniques using a 2-dimensional cross product. Compared with traditional approaches, the method yields better detection results in which the tampered regions are clearly identified. Another advantage is that the method can be applied to enhance a variety of detection algorithms. The method was tested on the CASIA TIDE v2.0 public dataset of color images and the results compared against those obtained using the re-interpolation, JPEG noise quantization and noise estimation techniques. The experimental results indicate that the proposed method is efficient and has superior detection characteristics.

Keywords: Image tampering, forgery detection, cross product

1. Introduction

The proliferation of low-cost, high-quality digital cameras and sophisticated image processing software make it very easy to manipulate or forge digital images without any obvious traces. Due to the dramatic increase in doctored images [1], the authenticity and trustworthiness of digital images are always in question. This situation can pose serious problems in criminal investigations, judicial proceedings, journalism, medical imaging and even insurance claim processing, where the authenticity of every digital image must be guaranteed.

A digital image may be tampered with via image retouching, splicing and/or copy-move forging. Retouching, cloning and healing are meth-

G. Peterson and S. Shenoi (Eds.): Advances in Digital Forensics XII, IFIP AICT 484, pp. 297–310, 2016.
DOI: 10.1007/978-3-319-46279-0_15

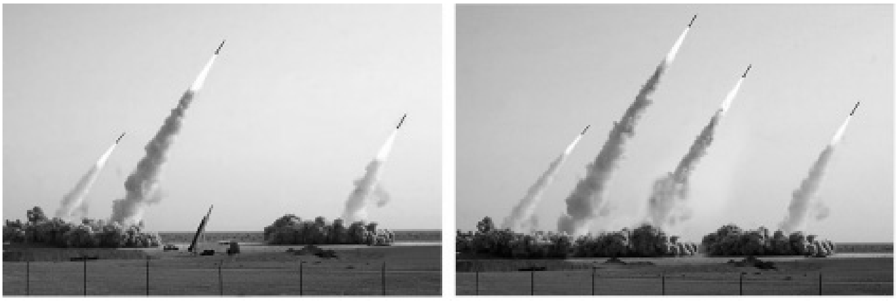

Figure 1. Original and forged images [1, 3].

ods of image manipulation in which some elements are removed, altered, blurred or emphasized using parts or properties of the same image; this type of manipulation also involves the adjustment of some image properties (e.g., color, white balance and contrast). Splicing [14] is a common image tampering technique; the technique combines image fragments from the same or different images to create a new image. Another popular technique for manipulating images is copy-move forgery [2]; this technique duplicates certain parts of a target image and places them elsewhere in the same image, the objective being to hide or emphasize parts of the target image. Figure 1 shows an original image (left) and its forged counterpart (right) [1, 3].

A number of researchers have studied the problem of image forgery detection. Zhao et al. [15] have leveraged JPEG compression characteristics to detect image inpainting in JPEG images. Kaur and Jyoti [7] have developed an image tampering detection method based on the inconsistency of JPEG grids in a suspect image. Cao et al. [2] have proposed an algorithm for detecting copy-move forgery using discrete cosine transforms and feature extraction. Talmale and Jasutkar [12] have evaluated a number of forgery detection methods. Birajdar and Mankar [1] have published a comprehensive survey of state-of-the-art passive techniques for detecting digital image forgeries.

In general, the image forgery detection techniques in the literature yield good results. However, in many cases, there is still a need for a human expert to make a final judgment about the detection results. The automation of this process can significantly reduce human effort in image forgery investigations.

This chapter proposes a new method for enhancing image forgery detection by combining two detection techniques using a 2-dimensional cross product. Compared with traditional approaches, the method yields better detection results in which the tampered regions are clearly iden-

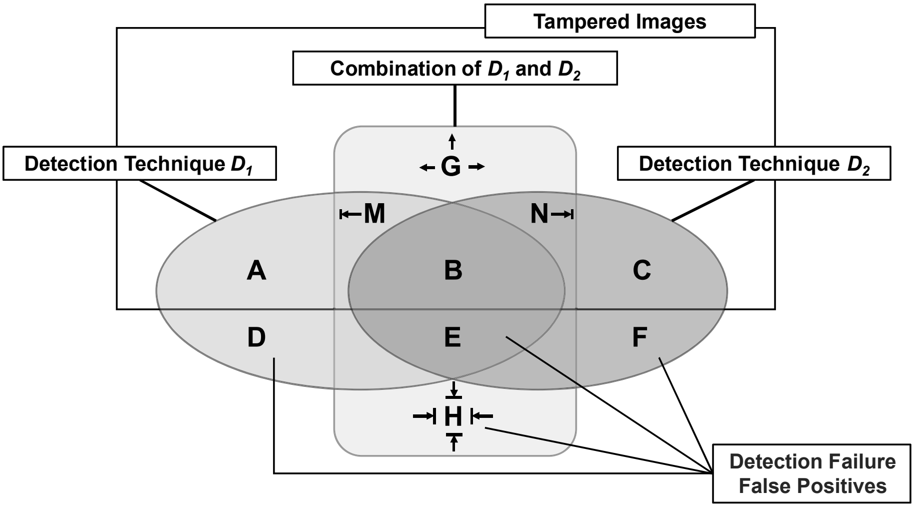
Tampered Images
Combination of D_1 and D_2
Detection Technique D_1
Detection Technique D_2
G
M
N
A
B
C
D
E
F
H
Detection Failure
False Positives

Figure 2. Proposed image forgery detection method.

tified. Another advantage is that the method can be applied to a wide variety of image forgery detection algorithms.

Figure 2 shows the conceptual idea underlying the proposed image forgery detection method. Specifically, two existing image forgery detection techniques D_1 and D_2 are combined. Regions A and C in the figure contain the tampered images that can be detected by techniques D_1 and D_2, respectively. Region B comprises the tampered images that both D_1 and D_2 can detect. In the case of detection failures, the false-positive results lie in the regions D, E and F.

When the proposed method is employed, tampered images that are detectable lie in regions B, M, N and G. The images in region G are the new tampered images that can be detected by combining techniques D_1 and D_2.

Due to the combination of techniques, the results are expected to be better than or at least equal to those contained in regions A, B and C. Hence, given regions M, N and G, the detection goal is to expand M and N to cover the A and C regions, and to expand G to cover additional tampered images.

A detection algorithm yields false-positive results when it determines that some authentic images have been tampered with. Thus, another important goal is to minimize the false-positive region H, ideally reduce it to null (empty). Unfortunately, the false-positive error problem is as yet unsolved and is the subject of ongoing research.

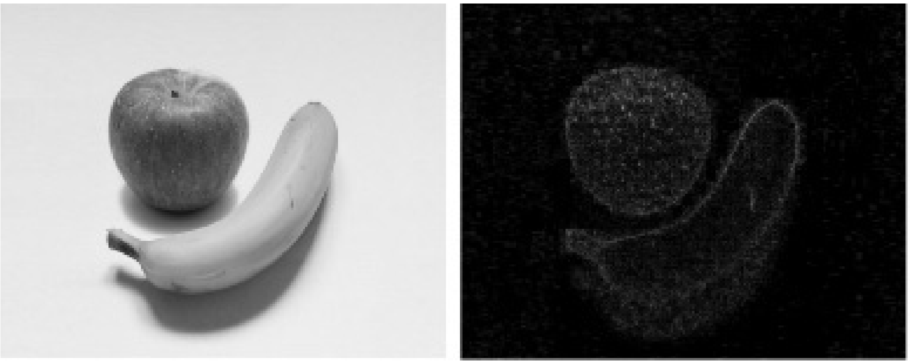

Figure 3. Applying error level analysis to a tampered JPEG image [3].

2. Related Work

A number of techniques have been proposed for detecting image tampering. The detection techniques can be divided into two categories: (i) active techniques; and (ii) passive techniques [1, 9]. Active detection techniques require additional information to be inserted into the target media at the time of creation (e.g., tags or watermarks); this information can be used to detect tampering in a suspect image. This research focuses on passive or blind techniques for detecting image tampering.

A passive detection technique requires no prior knowledge of the target image. One of the most popular passive forgery detection techniques leverages image noise inconsistency [8, 10]. The technique examines the level or variance of noise in a target image and searches for inconsistencies in the noise levels in different regions of the image.

Due to the quantization process, a JPEG image has the same level of information loss throughout the image. However, a tampered image may contain different levels of information loss. The error level analysis technique [4] attempts to identify image forgeries based on this idea. It determines image altering by re-saving a JPEG image and then subtracting the original image from the re-saved image. When the target image is re-saved, the quantization process is invoked once again on the target image. Thus, the image constructed by subtracting the original image from the re-saved image reveals the difference in compression (noise quantization) in the tampered regions. Figure 3 shows an example of applying an error level analysis technique to a tampered JPEG image (original tampered image (left) and detection image (right)).

However, in some cases, the image created by subtracting the original image from the re-saved image may not clearly distinguish the tampered regions. Such a situation requires a human expert to make the final de-

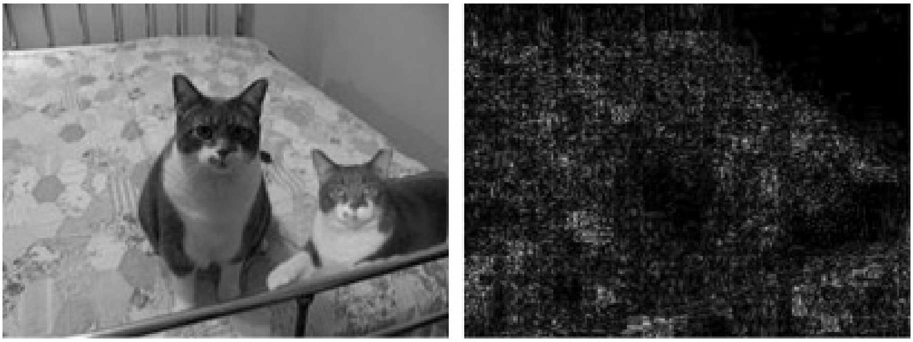

Figure 4. Failure of error level analysis on a tampered JPEG image [3].

cision regarding image forgery. Figure 4 shows an unsuccessful example of using an error level analysis technique on a tampered image (left). The detection image obtained by subtraction (right) is noisy and it is difficult to identify the tampered regions.

Image transformation and re-sampling are the most common techniques for altering images. These methods usually involve an interpolation process. Fortunately, the characteristics of an interpolated image can be leveraged to detect forgery.

A number of researchers have studied the use of interpolation characteristics to detect image tampering [5, 11, 13]. For example, Gallagher [5] has proposed a method to detect interpolation (i.e., linear and cubic interpolation) in compressed JPEG images using statistical analyses of digitally-enlarged images.

Hwang and Har [6] have proposed a novel technique for detecting forged images using a re-interpolation algorithm. They use characteristics obtained from a discrete Fourier transform conversion of a target image to determine the rate of interpolation. Normally, a higher interpolation rate in an image leads to a lower number of high frequency elements in the discrete Fourier transform conversion results. Using image scaling and a discrete Fourier transform, a detection map is created that enables the identification of the tampered regions. Figure 5 shows an example of applying the re-interpolation technique to a tampered JPEG image (original tampered image (left) and detection image (right)).

3. Proposed Method

This section describes the method for enhancing image forgery detection by combining two detection techniques. The method first applies the two image forgery detection techniques to a target image. Next,

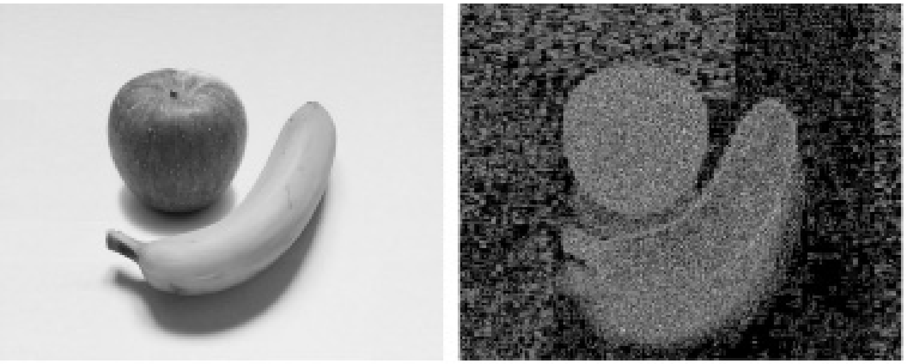

Figure 5. Applying a re-interpolation technique to a tampered JPEG image [3].

it combines the detection results obtained by each technique using a 2-dimensional cross product.

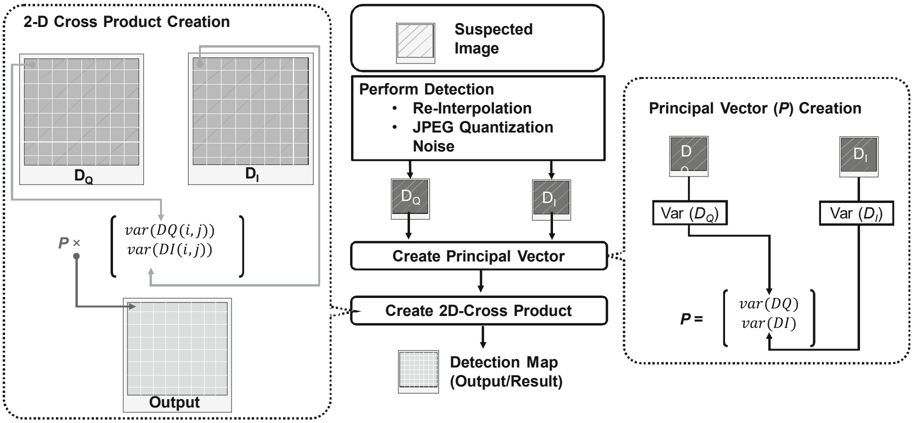

Figure 6. Overview of the proposed method.

Figure 6 presents an overview of the method. The goal is to combine two forgery detection techniques A and B on a target image I to obtain better results.

The proposed method involves the following steps:

- Techniques A and B are applied to the target image I to yield results R_A and R_B, respectively.

- The detection results R_A and R_B are used to create the principal vector $\vec{P}$.

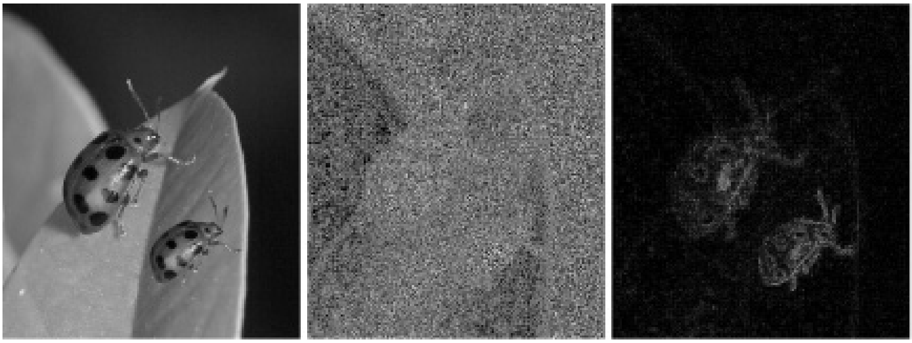

Figure 7. Detection using re-interpolation and JPEG noise quantization.

- The detection results R_A and R_B are divided into $m \times n$ fixed-size sub-blocks denoted by $R_A(i,j)$ and $R_B(i,j)$, where $1 \leq i \leq m$ and $1 \leq j \leq n$, respectively.

- A 2-dimensional cross product is performed of the principal vector $\vec{P}$ and every regional vector $V(i,j)$ created from the sub-blocks $R_A(i,j)$ and $R_B(i,j)$, where $1 \leq i \leq m$ and $1 \leq j \leq n$, respectively. This yields the enhanced detection result $D_E(i,j)$.

- $D_E(i,j)$ indicates the tampered regions in the target image I.

The image tampering detection method is implemented as a four-step procedure:

- **Step 1:** As shown in Figure 6, image forgery detection is enhanced by applying two detection techniques A and B in combination. First, image tampering detection is performed individually using techniques A and B:

$$R_{A,I} = D_A(I) \tag{1}$$

$$R_{B,I} = D_B(I) \tag{2}$$

  where $D_A(I)$ and $D_B(I)$ correspond to performing image tampering detection on the target image I using techniques A and B, respectively. The detection results are $R_{A,I}$ and $R_{B,I}$.

  Assume that detection technique A uses re-interpolation [6] while technique B uses JPEG noise quantization [4]. Figure 7 shows the corresponding detection results (original tampered image (left); re-interpolation detection image (center); and JPEG noise quantization detection image (right)).

- **Step 2:** The detection result images specified by Equations (1) and (2) are divided into $m \times n$ fixed-size rectangular sub-blocks. Let i and j be the row and column indices of the two result images. The sub-blocks of the two result images are expressed as $R_{A,I}(i,j)$ and $R_{B,I}(i,j)$, where $0 \leq i < m$ and $0 \leq j < n$.

- **Step 3:** A 2-dimensional cross product is performed on the result images $R_{A,I}$ and $R_{B,I}$. First, a principal vector $\vec{P}$ is created from $R_{A,I}$ and $R_{B,I}$ by computing the variance of each image:

$$\vec{P} = \begin{bmatrix} var(R_{A,I}) \\ var(R_{B,I}) \end{bmatrix} \tag{3}$$

- **Step 4:** Having created the principal vector, regional vectors $\vec{V}(i,j)$ are created for each sub-block of $R_{A,I}$ and $R_{B,I}$:

$$\vec{V}(i,j) = \begin{bmatrix} var(R_{A,I}(i,j)) \\ var(R_{B,I}(i,j)) \end{bmatrix} \tag{4}$$

- **Step 5:** The 2-dimensional cross product is performed of the principal vector $\vec{P}$ and every regional vector $\vec{V}(i,j)$ to yield the result matrix $M(i,j)$:

$$M(i,j) = \vec{P} \times \vec{V}(i,j) \tag{5}$$

- **Step 6:** The result matrix $M(i,j)$ is plotted to view the enhanced detection results.

Figure 8 compares the results obtained using the original techniques and those obtained using the proposed method (original tampered image (top left); re-interpolation detection image (top right); JPEG noise quantization detection image (bottom left); and proposed method detection image (bottom right)). The results show that the proposed method accurately extracts the tampered regions (i.e., two lady bugs) from the non-tampered regions compared with the original techniques (i.e., re-interpolation and JPEG noise quantization). The improvement in image tampering detection is beneficial to security and forensic practitioners as well to non-expert personnel who conduct image forgery investigations.

4. Experimental Results

The experiments used the CASIA TIDE v2.0 [3] public dataset consisting of 7,491 authentic and 5,123 tampered color images. The authentic and tampered image sizes varied from small (240×160 pixels) to

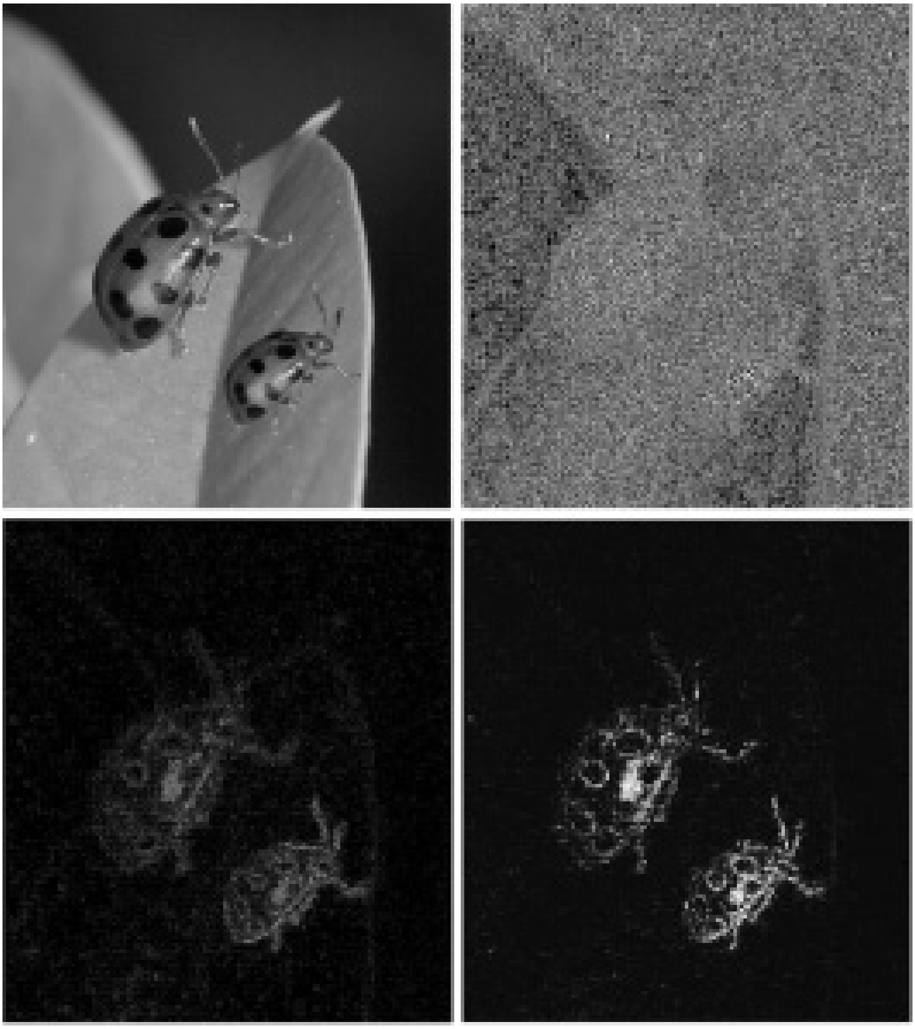

Figure 8. Comparison of detection results.

large (900 × 600 pixels). The sizes of the tampered regions within each forged image varied considerably.

The experiments focused on JPEG images. The proposed method was applied to three image tampering techniques: (i) re-interpolation; (ii) JPEG noise quantization; and (iii) noise estimation. Thus, three combinations of two techniques were employed: (i) re-interpolation with JPEG noise quantization; (ii) re-interpolation with noise estimation; and (iii) JPEG noise quantization with noise estimation.

Re-interpolation usually produces pattern mismatches between the forged and non-forged regions of a target image. However, it can be extremely difficult to precisely locate the tampered regions in the target image.

JPEG noise quantization can efficiently locate the tampered regions in a target image. However, this technique usually produces some irrelevant noise that can hinder the identification of forged images.

Noise estimation gives a result image that indicates the noise levels across a target image. Using the result image, it is possible to locate the tampered regions by considering the differences in the noise levels. However, in situations where the noise levels in the tampered and non-tampered regions are close to each other, it is difficult to detect forgeries and/or erroneous results may be obtained. Even human experts may have difficulty in precisely locating the tampered regions in a target image.

Figure 9 compares the results obtained by applying the three image tampering detection techniques individually with those obtained by applying them in combination using the proposed method. Specifically, Figure 9 shows the results obtained for four tampered images (larger images on the extreme left of the four rows). The smaller images to the right of each original image correspond to: top row (left to right) – re-interpolation detection image, JPEG noise quantization detection image and noise estimation detection image; and bottom row (left to right) – re-interpolation with JPEG noise quantization detection image, re-interpolation with noise estimation detection image and JPEG noise quantization with noise estimation detection image. The results show that the proposed method produces much better results than the individual techniques. Indeed, the proposed method yields improved clarity, enabling the tampered regions to be explicitly differentiated from other parts of the images.

Figure 10 shows an unsuccessful result obtained using the proposed method. The results indicate that only one tampered region exists – the yellow ribbon in the upper portion of the target image. JPEG noise quantization (top row) and noise estimation (bottom row) both produce false-positive results, incorrectly identifying non-tampered regions as tampered regions. The re-interpolation technique results show pattern inconsistencies in the yellow ribbon region as well as in the remainder of the target image. Indeed, the result is very noisy and cannot be used to accurately locate the tampered region (i.e., yellow ribbon). The reason is that the conventional detection techniques yield incorrect results. As a result, the proposed method, which combines the two

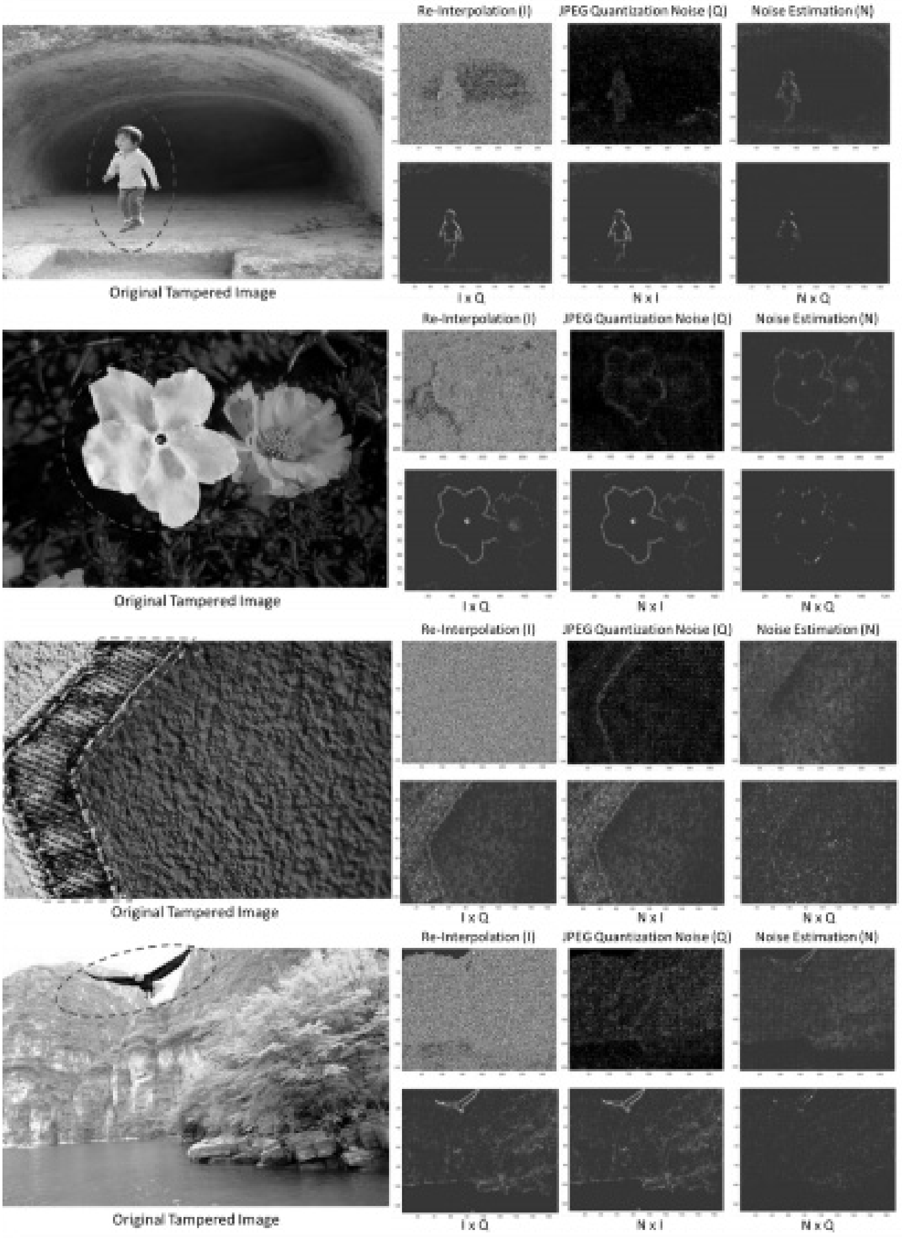

Figure 9. Comparison of detection results.

conventional techniques using a 2-dimensional cross product, also yields incorrect results.

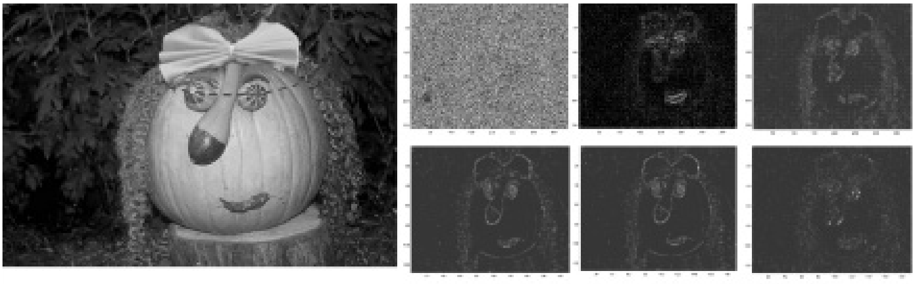

Figure 10. Unsuccessful result.

5. Discussion

The experimental results demonstrate that the combination of two passive detection methods can enhance image tampering detection. In particular, the clarity of a detection image is improved and the tampered regions are more easily distinguished from the non-tampered regions. The proposed method can be applied to any passive detection techniques that find inconsistencies in image properties (e.g., noise, color temperature and compression noise).

The proposed method suffers from some drawbacks. The main drawback is that, if the two tampering detection techniques that are combined produce noisy results or false-positive errors, then the results produced by the proposed method are affected negatively. Another challenge is to find the appropriate principal vector and regional vectors. The principal vector expresses the combination of the result images produced by the two tampering detection techniques. Regional vectors represent blocks of the two result images. Thus, performing 2-dimensional cross products of the principal and regional vectors essentially yields the differences between the principal vector and each regional vector. Creating principal and regional vectors based on simple variance calculations may not accurately represent the entire result images (in the case of the principal vector) and each portion of the result images (in the case of the regional vectors).

6. Conclusions

The proposed method for image forgery detection combines two conventional passive detection techniques using a 2-dimensional cross product. The method can employ any passive detection techniques that find inconsistencies in target image properties (e.g., noise, color temperature and compression noise). Experimental results indicate that the method is efficient and has superior detection characteristics than when each passive detection technique is used individually. In particular, the clarity of the detection images are improved, enabling the tampered regions to be distinguished from the non-tampered regions more easily. The improvement in tampered image detection is beneficial to security and forensic practitioners as well to non-expert personnel who conduct image forgery investigations. Another advantage is that the proposed method is readily automated, potentially reducing the human effort involved in image forgery investigations.

The principal drawback of the method is that its results are dependent on the results produced by the individual detection techniques. Another problem is posed by creating the principal vector and regional vectors using simple variance calculations; this potentially affects the fidelity of image representations and, consequently, the detection results. Future research will attempt to enhance the proposed image forgery detection method by addressing these two limitations.

References

[1] G. Birajdar and V. Mankar, Digital image forgery detection using passive techniques: A survey, *Digital Investigation*, vol. 10(3), pp. 226–245, 2013.

[2] Y. Cao, T. Gao, L. Fan and Q. Yang, A robust detection algorithm for copy-move forgery in digital images, *Forensic Science International*, vol. 214(1-3), pp. 33–43, 2012.

[3] Chinese Academy of Sciences Institute of Automation (CASIA), CASIA v2.0, Beijing, China (`forensics.idealtest.org/casiav2`), 2016.

[4] H. Farid, Exposing digital forgeries from JPEG ghosts, *IEEE Transactions on Information Forensics and Security*, vol. 4(1), pp. 154–160, 2009.

[5] A. Gallagher, Detection of linear and cubic interpolation in JPEG compressed images, *Proceedings of the Second Canadian Conference on Computer and Robot Vision*, pp. 65–72, 2005.

[6] M. Hwang and D. Har, A novel forged image detection method using the characteristics of interpolation, *Journal of Forensic Sciences*, vol. 58(1), pp. 151–162, 2013.

[7] M. Kaur and Jyoti, Image tamper detection using non alignment of JPEG grids, *International Journal of Emerging Technologies in Computational and Applied Sciences*, vol. 6(4), pp. 331–333, 2013.

[8] B. Mahdian and S. Saic, Using noise inconsistencies for blind image forensics, *Image and Vision Computing*, vol. 27(10), pp. 1497–1503, 2009.

[9] B. Mahdian and S. Saic, A bibliography on blind methods for identifying image forgery, *Signal Processing: Image Communication*, vol. 25(6), pp. 389–399, 2010.

[10] X. Pan, X. Zhang and S. Lyu, Exposing image forgery with blind noise estimation, *Proceedings of the Thirteenth ACM Workshop on Multimedia and Security*, pp. 15–20, 2011.

[11] A. Popescu and H. Farid, Exposing digital forgeries in color filter array interpolated images, *IEEE Transactions on Signal Processing*, vol. 53(10), pp. 3948–3959, 2005.

[12] G. Talmale and R. Jasutkar, Analysis of different techniques of image forgery detection, *IJCA Proceedings on National Conference on Recent Trends in Computing*, vol. 2012(3), pp. 13–18, 2012.

[13] Y. Yun, J. Lee, D. Jung, D. Har and J. Choi, Detection of digital forgeries using an image interpolation from digital images, *Proceedings of the IEEE International Symposium on Consumer Electronics*, 2008.

[14] Z. Zhang, Y. Zhou, J. Kang and Y. Ren, Study of image splicing detection, *Proceedings of the Fourth International Conference on Intelligent Computing*, pp. 1103–1110, 2008.

[15] Y. Zhao, M. Liao, F. Shih and Y. Shi, Tampered region detection of inpainted JPEG images, *Optik – International Journal for Light and Electron Optics*, vol. 124(16), pp. 2487–2492, 2013.