Image Splicing Localization Based on Re-demosaicing*

Bo Wang and Xiangwei Kong

School of Information and Communication Engineering,
Dalian University of Technology, Dalian, P.R. China
{bowang,kongxw}@dlut.edu.cn

Abstract. Image splicing is the most fundamental step of photomontage. In this paper, we propose an efficient blind digital forensics method for image splicing localization. In our method, the demosaicing is used for estimating the natural counterpart of spliced image, which is compared with the test image to expose the abrupt edges along the spliced region. According to the smoothness comparison results, we obtain a binary image to illustrate the localization of the splicing. To evaluate the performance of our method, we apply this approach to DVMM uncompressed spliced image database, and the experimental results indicate the effectiveness on splicing localization.

Keywords: digital image forensics, image splicing, splicing localization, re-demosaicing.

1 Introduction

Photomontage, with a history as long as photography, has become a new serious problem in the digital epoch. In analog image period, creating an image forgery requires sophisticated technique of dark room manipulations, while in recent years digital cameras and high performance photo editing software have made it easy for amateurs to produce digital image forgeries. As a result, the increasing forgeries transmitted via the Internet have a negative impact on many aspects of the society, such as the perception of the public trust. A typical example is the famous picture widely spread on the Internet before the presidential year 2004 in United States, which shows that John Kerry and Jane Fonda's presences at an anti-war rally. The picture with obvious political purpose impacted John Kerry's political life more or less, while a later report had indicated that this photo was a spliced forgery.

In recent years, more and more image forgeries that appear on the Internet and public media confuse the public trust. This situation makes an urgent demand on solutions for detecting the authentication of digital images. Digital image forensics provides a blind and passive approach without embedding advance information in images. Many researchers have paid more attention on digital image forensics.

To automatically expose potential spliced image forgery, many efforts have been made for passive and blind splicing detection during the past few years [1,2]. For detecting the duplicated regions in forged images, two methods are respectively

* This work is supported by the National Natural Science Foundation of China under Grant No. 60971095, and also the Fundamental Research Funds for the Central Universities.

D. Zeng (Ed.): Advances in Information Technology and Industry Applications, LNEE 136, pp. 725–732.
springerlink.com

proposed in [3] and [4] by computing the correlations of the fixed size image blocks. H. Farid [5] proposed an approach to expose image manipulations including image splicing based on a statistical model of "natural" image. In [6-8], he also provided us a method to detect spliced images using image lighting inconsistency. T. T. Ng et al. [9] proposed an image splicing model based on the idea of bipolar signal perturbation, and they used bicoherence features to detect spliced forgery [10]. W. Chen et al. [11,12] have introduced 2-D phase congruency and statistical moments of characteristic function to digital forensics. In [13], geometry invariants and camera characteristics consistency are used to detect spliced images. The SIFT is applied to detect image forgeries [14, 15]. Besides, several physical characteristics [16-21] introduced by components of image pipeline have been used for splicing detection.

Besides, the forensic analyst often concerns more about where the spliced region is and which objects in the image are pasted. Y. F. Hsu and S. F. Chang [22] recently proposed a method based on camera function consistency to detect image splicing. The results indicate that an incomplete localization of spliced region is achieved. However, the factors of empirical segmentation number and the texture of images etc. usually impact the detection accuracy.

In this paper, we propose an approach for image splicing localization. By using re-demosaicing, we obtain a natural counterpart estimation of the test image. After a comparison of smoothness between the test image and its estimated one, the algorithm provides credible localization of the spliced region. The experimental results on the publicly available database from DVMM [23] show that our method can localize the spliced region in a high accuracy.

The rest of this paper is organized as follows. A simple and quick review of image formation pipeline is introduced in Section 2. In Section 3, the method of estimating the natural counterpart of test image is proposed, followed by the description that how to localize the spliced region. Section 4 provides the details of the experiments, and discussions are furthermore given. The paper is summarized finally in Section 5.

2 Image Formation Pipeline in Digital Camera

The image formation pipeline is illustrated in Figure 1. For most consumer-end cameras, there is a color filter array (CFA) placed before the sensor. The CFA is carefully designed according to HVS. Typical CFA, which is called Bayer CFA, consists of several 2×2 basic units including one red, one blue and two green components, as Figure 2 illustrated.

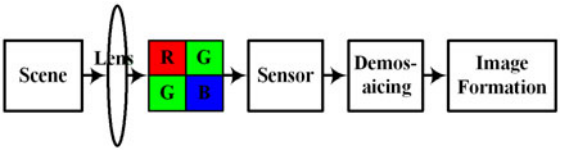

Fig. 1. Image formation pipeline

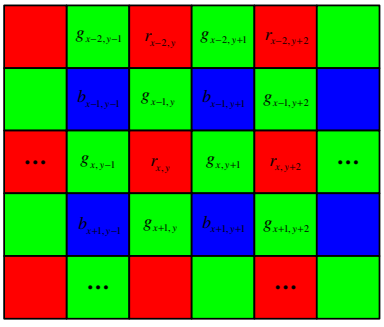

Fig. 2. Bayer CFA

Obviously, the digital signal in each pixel is the intensity of one of three colors, sampled by the CFA. To obtain a RGB colorful image, the missing two color components in each pixel are demosaiced by interpolation algorithm using the neighbor sampled pixel values. This important step in image formation pipeline is called demosaicing. There are various demosaicing algorithms, and different camera makers employ different demosaicing methods. Generally, we can divide these methods into two categories, as non-adaptive and adaptive algorithms.

Typical non-adaptive algorithms, such as bilinear and bicubic [24], act on each channel independently. These kernel-based demosaicing algorithms can be modeled with a low-pass filter, and usually present good performance in smooth regions because of the low-pass filter characteristics.

Considering the texture of image, the adaptive demosaicing algorithms usually classify pixels into several categories, and use different interpolation methods. Typical adaptive algorithms include gradient-based [25], ACP [26] and TBVNG [27] methods. Because of the limited length of this paper, we would not describe the detail of these methods. More elaborate description will be found in [25-27].

3 Proposed Method

Figure 3 illustrates the framework of our method, including three steps to localize the image splicing. By re-sampling the image in Bayer CFA manner and re-demosaicing, we obtain the estimated "natural" one. After that, a comparison between the test image and its natural counterpart is applied to classify each pixel as authentic pixel or forgery one. According to the classification results, a binary image with the same size of the test image is generated, which indicates the spliced edges after a post-processing. In the following subsections, all of these steps will be described in detail.

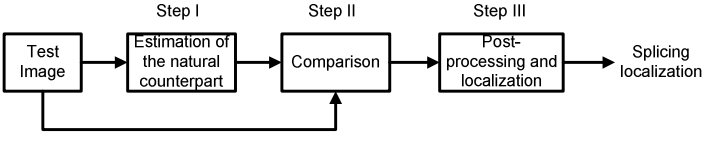

Fig. 3. The framework of proposed method

3.1 Estimate the Natural Counterpart of the Suspect Image

For a practical scenario, only the suspect image for test is available. If we obtain a natural counterpart of the test image, the spliced forgery will show obvious differences between itself and the estimated counterpart along the spliced edge, because the abrupt changes are introduced by the splicing. While for the authentic image, the estimated counterpart will be approximately similar with the test image. Having noticed that, a good performance estimation of the natural counterpart for the test image is required.

We estimate the natural counterpart of the suspect image by CFA re-sampling and re-demosaicing. The re-demosaicing of the suspect image will help us to reconstruct the continuity for the estimated natural counterpart. To obtain a good estimation of the natural counterpart of the test image, the CFA re-sampling pattern and demosaicing algorithm needs to be selected carefully.

Without restricting generality, we adopt the most popular Bayer CFA as the re-sampling pattern, as Figure 2 illustrated. The other factor is demosaicing algorithm. There are several methods nowadays. In terms of non-adaptive methods, an effect similar to a low-pass filter is usually introduced due to the kernel of demosaicing function, therefore resulting in significant blurring along edge regions. In this case, a relative bigger variance may lead to a false positive alarm in comparison. However, the complex adaptive demosaicing methods usually keep the discontinuity in spliced images. As a result, the comparison would expose a few differences between the test image and its counterpart, and therefore classifying the forged image as an authentic one, which is called false negative.Considering the balance of false positive and negative, we adopt gradient-based demosaicing [25] as the interpolating method to estimate the "natural" image based on the analysis above.

Given a $M \times N$ suspect RGB color image I_t, we present it as equation (1):

$$I_t = \left\{ p_{x,y,k} \,\middle|\, x \in [1, M],\ y \in [1, N],\ k \in \{R, G, B\} \right\} \tag{1}$$

where $p_{x,y,k}$ denotes each single pixel in the image, and R, G and B indicate the red, green and blue component respectively. The equation (2) and Figure 4 show the process of how to estimate the natural counterpart I'_t.

$$I'_t = f_{gb}\left(f_{cfa}\left(I_t\right)\right) \tag{2}$$

where $f_{gb}(\cdot)$ and $f_{cfa}(\cdot)$ denote gradient-based demosaicing method [25] and the Bayer CFA sampling.

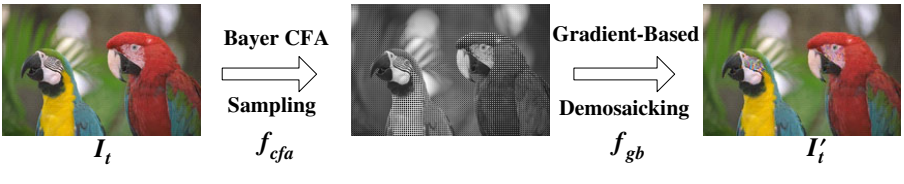

Fig. 4. Flow of the natural counterpart estimation in our method

3.2 Comparison

We use the absolute value of the difference between the test image and its counterpart for the comparison. For each pixel, three distances are computed respectively for red, green and blue component, as equation (3) indicates:

$$d_{x,y,k} = \left| p_{x,y,k} - p'_{x,y,k} \right|_{x\in[1,M],y\in[1,N],k\in\{R,G,B\}} \tag{3}$$

Each distance is used to compare with a threshold $T_k, k \in \{R,G,B\}$ calculated by equation (4). The threshold is the combination of an empirical factor α and the max difference between the neighbor pixels, along four directions, horizon, vertical and diagonal. For the three-color components, we classify the suspect pixels as spliced pixels in our method, if any distance of these three exceeds the threshold.

$$T_k = \alpha \times \max\left(\left| p_{x-1,y,k} - p_{x+1,y,k} \right|, \left| p_{x,y-1,k} - p_{x,y+1,k} \right|, \left| p_{x-1,y-1,k} - p_{x+1,y+1,k} \right|, \left| p_{x-1,y+1,k} - p_{x+1,y-1,k} \right| \right) \tag{4}$$

$$p_{x,y} = \begin{cases} 1, & Spliced, if \exists d_{x,y,k} > T_k \\ 0, & Authentic, if \forall d_{x,y,k} \le T_k \end{cases} \tag{5}$$

The parameter α, which balances the positive and false negative alarm of detection, is experimentally determined as 0.9.

In the output of the comparison, a binary image I_r with the same resolution of the test image is obtained to indicate the spliced pixels using 0 and authentic pixels with 1.

3.3 Post-processing for Splicing Localization

In our analysis of the primary result I_r, we find that there are some authentic pixels misclassified as spliced ones usually occurring in smooth area. We owing this to two reasons: One can be explained by the magnified bias between test pixel and its estimated version. After re-demosaicing, we have to round off the pixel value to integer to obtain the nature counterpart image. This operation sometimes will magnify the bias that is then possibly analogous with the threshold. We call this kind of points "flat pixel". The other reason is the noise. The noisy points usually present discontinuity with the neighborhood, like the spliced pixels.

Considering the flat pixel, we employ an edge detection algorithm to remove the positive false points in the raw result. In our method, a reasonable assumption is that the spliced pixels are the edge pixels. Based on this assumption, canny edge detector is applied in our method. After the canny edge detection of the test image, an operation of logical AND is applied to the edge detection result and the raw result I_r. We denote the results of this operation as $I_{r\text{-}e}$. The application of edge detection method can effectively solve the problem of flat pixels.

For the purpose of reducing the effect of the noisy pixels, we design a filter for $I_{r\text{-}e}$. The filter works in the following manner. In each 3×3 block of the $I_{r\text{-}e}$, if there are at least two adjacent spliced pixels marked as 1, for example as Figure 5(a) illustrated, the spliced pixels in the block will be regarded as real forgeries, otherwise the spliced pixels are considered as false positive and re-marked as 0, as Figure 5(b) and 5(c). In the output of the filter $I_{r\text{-}e\text{-}f}$, most of the false positive alarms caused by the noisy pixels will be eliminated.

Fig. 5. Samples of (a): real forgery block and (b), (c): false positive alarms caused by noisy pixels

The binary image $I_{r\text{-}e\text{-}f}$ that we finally obtained localizes the spliced edge with white points and authentic pixels with black.

4 Experiments and Discussions

The image dataset used in our experiment for evaluating the performance of the proposed method is provided by DVMM [23]. The open authentic/spliced image dataset consists of 183 authentic images and 180 spliced images, with resolution varied from 757×568 to 1152×768. All of the authentic images are taken by 4 cameras. Each spliced image is created in Adobe Photoshop, by pasting an authentic image with visually salient objects, which is copied from another image taken by a different camera. No post-processing was performed. As 30 images are created for each camera pair, total of $P_4^2 \times 30 = 180$ images is obtained. All of the authentic and spliced images are uncompressed saved in TIFF format. The (a) and (c) columns of Figure 6 illustrate samples of the authentic and spliced forgeries.

The localization results are illustrated in Figure 6(b) and 6(d) column. For the authentic images, no evident spliced edge in the binary image is exposed, though false positive alarm occurs at some pixels. The detecting results of spliced forgeries, however, show obvious contour of the pasted object with the edges in white.

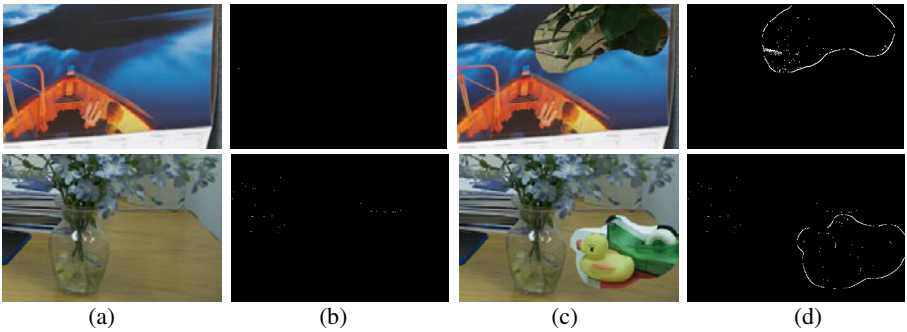

Fig. 6. Sample of authentic images and spliced forgeries in our experiments: (a) authentic images; (b) detection result of (a); (c) spliced forgeries and (d) localization results of (c)

5 Conclusions

In this paper, we propose a novel approach to localize spliced area, by introducing re-demosaicing in authentic counterpart estimation of a spliced image for the first time. The combination of Bayer CFA and gradient-based interpolation algorithm is employed as the estimator. A straightforward comparator is applied to the pair of images, and a binary image is obtained as the result. By a post-processing of the result, we finally get the binary image to localize the spliced area. The experimental results of DVMM image dataset indicate the precise of our method in splicing localization.

References

1. Christlein, V., Riess, C., Angelopoulou, E.: A Study on Features for the Detection of Copy-Move Forgeries. In: Information Security Solutions Europe, Belin, Germany (2010)
2. Farid, H.: A Survey of Image Forgery Detection. IEEE Signal Processing Magazine 2(26), 16–25 (2009)
3. Fridrich, J., Soukal, D., Lukáš, J.: Detection of copy-move forgery in digital images. In: Digital Forensic Research Workshop (August 2003)
4. Popescu, A., Farid, H.: Exposing digital forgeries by detecting duplicated image regions. Technical Reports TR2004-515, Dartmouth College (August 2004)
5. Farid, H.: A picture tells a thousand lies. New Scientist 179(2411), 38–41 (2003)
6. Johnson, M., Farid, H.: Exposing digital forgeries by detecting inconsistencies in lighting. In: ACM Multimedia and Security Workshop, pp. 1–9. ACM, New York (2005)
7. Kee, E., Farid, H.: Exposing Digital Forgeries from 3-D Lighting Environments. In: Workshop on Information Forensics and Security. IEEE Press, Seattle (2010)
8. Johnson, M., Farid, H.: Exposing Digital Forgeries in Complex Lighting Environments. IEEE Transactions on Information Forensics and Security 3(2), 450–461 (2007)
9. Ng, T.-T., Chang, S.-F.: A model for image splicing. In: IEEE International Conference on Image Processing, pp. 1169–1172. IEEE Press, Singapore (2004)
10. Ng, T.-T., Chang, S.-F.: Blind detection of photomontage using higher order statistics. In: IEEE International Symposium on Circuits and Systems, pp. 688–691. IEEE Press, Canada (2004)
11. Chen, W., Shi, Y.Q., Su, W.: Image splicing detection using 2-D phase congruency and statistical moments of characteristic function. In: SPIE Electronic Imaging. SPIE Press, San Jose (2007)
12. Shi, Y.Q., Chen, C., Chen, W.: A natural image model approach to splicing detection. In: ACM Multimedia and Security Workshop, pp. 51–62. ACM, Dallas (2007)
13. Hsu, Y.-F., Chang, S.-F.: Detecting image splicing using geometry invariants and camera characteristics consistency. In: IEEE International Conference Multimedia & Expo, Toronto, pp. 549–552. IEEE Press, Canada (2006)
14. Xunyu, P., Siwei, L.: Detecting Image Region Duplication Using SIFT Features. In: International Conference on Acoustics, Speech, and Signal Processing, pp. 1706–1709. IEEE Press, Dallas (2010)
15. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A., Serra, G.: Geometric Tampering Estimation by Means of a SIFT-based Forensic Analysis. In: International Conference on Acoustics, Speech, and Signal Processing, pp. 1702–1705. IEEE Press, Dallas (2010)

16. Lukáš, J., Fridrich, J., Goljan, M.: Detecting digital image forgeries using sensor pattern noise. In: SPIE Electronic Imaging, pp. 362–372. SPIE Press, San Jose (2006)
17. Chen, M., Fridrich, J., Goljan, M., Lukáš, J.: Determining image origin and integrity using sensor noise. IEEE Transaction on Information Security and Forensics 3(1), 74–90 (2008)
18. Huang, Y.: Can digital image forgery detection be unevadable? A case study: color filter array interpolation statistical feature recovery. In: SPIE Visual Communications and Image Processing, pp. 980–991. SPIE Press, Beijing (2005)
19. Ng, T.-T., Chang, S.-F., Tsui, M.-P.: Using geometry invariants for camera response function estimation. In: IEEE International Conference on Computer Vision and Pattern Recognition, pp. 1–8. IEEE Press, Minneapolis (2007)
20. Lin, Z., Wang, R., Tang, X., Shu, H.-Y.: Detecting doctored images using camera response normality and consistency. In: IEEE International Conference on Computer Vision and Pattern Recognition, pp. 1087–1092. IEEE Press, San Diego (2005)
21. Fu, D., Shi, Y.Q., Su, W.: Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition. In: 5th International Workshop on Digital Watermarking, pp. 177–187. IEEE Press, Korea (2006)
22. Hsu, Y.-F., Chang, S.-F.: Image splicing detection using camera response function consistency and automatic segmentation. In: IEEE International Conference on Multimedia & Expo, pp. 28–31. IEEE Press, Beijing (2007)
23. Columbia Uncompressed Image Splicing Detection Evaluation Dataset, `http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataplicedDataSet/uthSplicedDataSet.htm`
24. Keys, R.G.: Cubic convolution interpolation for digital image processing. IEEE Transactions on Acoustics, Speech, and Signal Processing, ASSP 29(6), 1153–1160 (1981)
25. Laroche, C.A., Prescott, M.A.: Apparatus and method for adaptively interpolating a full color image utilizing chrominance gradients. US Patent, 5373322 (1940)
26. Hamilton, J.F., Adams, J.E.: Adaptive color plane interpolation in single sensor color electronic camera. US Patent, 5629734 (1997)
27. Chang, E., Cheung, S., Pan, D.Y.: Color filter array recovery using a threshold-based variable number of gradients. In: Sensors, Cameras, and Applications for Digital Photography, vol. 3650, pp. 36–43. IEEE Press (1999)