

IMAGE SPLICING DETECTION BASED ON DEMOSAICKING AND WAVELET TRANSFORMATION

Endina Putri Purwandari

Informatics Engineering Department, Engineering Faculty, University of Bengkulu, Jl. WR. Supratman
Kandang Limun, Bengkulu 38371, Indonesia

E-mail: endinaputri@unib.ac.id

Abstract

Image splicing is a form of digital image manipulation by combining two or more image into a new image. The application was developed through a passive approach using demosaicking and wavelet transformation method. This research purposed a method to implement the demosaicking and wavelet transform for digital image forgery detection with a passive approach. This research shows that (1) demosaicking can be used as a comparison image in forgery detection; (2) the application of demosaicking and wavelet transformation can improve the quality of the input image (3) demosaicking and wavelet algorithm are able to estimate whether the input image is real or fake image with a passive approach and estimate the manipulation area from the input image.

Keywords: *demosaicking, wavelet transform, image splicing, digital image manipulation*

Abstrak

Penggabungan citra adalah bentuk manipulasi citra digital dengan cara menggabungkan dua atau lebih citra menjadi sebuah citra baru. Aplikasi dikembangkan melalui pendekatan pasif menggunakan metode *demosaicking* dan transformasi *wavelet*. Tujuan penelitian ini adalah memberikan metode dalam implementasi *demosaicking* untuk deteksi pemalsuan citra digital dengan pendekatan pasif. Penelitian ini menunjukkan bahwa (1) citra *demosaicking* dapat menjadi citra pembandingan dalam deteksi pemalsuan; (2) penerapan kombinasi algoritma *demosaicking* dan transformasi *wavelet* telah dapat meningkatkan kualitas citra masukan; (3) Algoritma *demosaicking* dan *wavelet* dengan pendekatan pasif telah dapat memperkirakan citra input adalah citra asli atau palsu dan memperkirakan wilayah citra masukan yang telah mengalami manipulasi digital.

Kata Kunci: *demosaicking, transformasi wavelet, image splicing, manipulasi citra digital*

1. Introduction

Digital world has been growing rapidly such as the existence of high technology computers, digital cameras, and image manipulation software. The image forgery trend have changed from analog to digital techniques using computer software, graphics software, and digital cameras. Availability of image manipulation software package such as Adobe Photoshop and Gimp that make images can be modified easily. It enables a high technology digital image manipulation process by every user even for unprofessional users.

Some time ago, Bengkulu shocked by the spread of immoral photo. Photographs and conversations recording were spread through BlackBerry Messenger (BBM), between a woman's status as the wife with a man who as the Bengkulu officials [1]. Various assumptions were spread in community to authenticate the photos. Therefore, it is necessary to develop software system for im-

age forgery detection that can determine the authenticity of the digital image effectively and efficiently.

Image forgery detection method is divided into two approaches, there are active (non-blind) and passive (blind) image forensics. Active approach is done by inserting a signature (digital signature) and the watermark (digital water-marking) in the digital image [2]. However this requires additional hardware, thus most imaging devices do not carry this function. The passive approach is a form of new research in the area of digital multimedia different security with an active approach. Image forensics makes use of the characteristics of the imaging devices and the properties of digital images to test whether images in question are authentic in particular they have been manipulated.

Digital image forgery is an image that has undergone manipulation on changes to the content and/or context. Farid [3] divides the image into

two categories counterfeiting, which changes the content (content alteration) and changes in context (context alteration). The manipulation of context changes cause a shift of meaning that one of the specific part image or the entire image. Changes that occur in the context of the image can be determined by answering the questions who, what, when, where and when to that image. Generally, the context changes aim to add dramatic impact and shifting public opinion against a particular object in the image.

Forms of image forgery category content changes [4] consists of: (1) Duplication region (duplicated region); (2) Merger image (image splicing); (3) Elimination (deletion); (4) Changing the size (resizing); and (5) Improved image quality (general enhancement). Among all the image manipulation operations, image splicing is a common operation on the digital image forgery [5]. Splicing operation is done by copying and pasting parts of the image from one or more images to another image. This procedure resulted changes and differences in consistency, continuity, and the correlation between image pixels.

Hsu and Chang [6] check the consistency of camera characteristics among different areas in an image. Chen et al [7] extract features from the sharp transitions introduced by the spliced image part, their features mainly comes from the moments of wavelet characteristics functions and 2D phase congruence. Shi et al [8] extract features from moments of characteristics function of wavelet sub-band and Markov transition probabilities.

A color image requires at least three color samples at each pixel location. Computer images often used red (R), green (G), and blue (B). In a three-chip color camera, the light entering camera is split and projected onto each spectral sensor. Thus, many digital cameras use a single-chip Charge Coupled Device (CCD) covered with a Color Filter Array (CFA). The CFA must be placed between the lens and the sensors for digital acquisition of color images. One of the most widely used CFA patterns is the Bayer mosaic pattern. To render full resolution images, the missing color information must be estimated from the surrounding pixels, commonly referred to as CFA demosaicking.

The CFA pattern estimation method used in this work was first introduced by Dirik [9] to distinguish real images from computer generated (CG) ones. Here, we apply the method to the tamper detection problem. The second method, CFA based noise analysis, relies on the fact that sensor noise power in CFA interpolated pixels should be significantly lower than non-interpolated pixels due to the low pass nature of CFA demosaicking. In Gallagher [10], a similar approach was used to

capture CFA traces to distinguish CG from real images by high pass filtering and Fourier analysis.

Image authentication process is still a new challenge in proving the authenticity of the image. In this paper, we propose a new blind and effective the development of image splicing applications for image forgery detection. This application is done through passive approach using demosaicking and wavelet transformation.

2. Methods

Demosaicking Method

The key part of any digital camera is CCD/CMOS sensor, which transform light signals into electric ones. Because all these sensors are sensitive to the light energy, thus to generate a colourful image, most cameras employ a Color Filter Array (CFA) overlaid on the sensor. To build the full color image, the missing values are interpolated from the neighborhood available sensor readings. This interpolation process is often referred to as demosaicking. Demosaicking scheme aims to make reconstruction once again in input image using Bayer pattern which is considered as information from image of CFA sensor result on digital cameras. In CFA interpolation scheme, Bayer layer of the third RGB color channels will be interpolated again with matrix convolution H_r , H_g , and H_b . Furthermore, Bayer layer calculation with convolution matrix produces an interpolation image in overall RGB channel [11], as shown in Figure 1. A bayer pattern is arranged in a square grid of photo sensors, arranged in 50% green, 25% red, and 25% blue square block, and two green values must lie diagonally.

On RGB calculation for bilinear algorithm

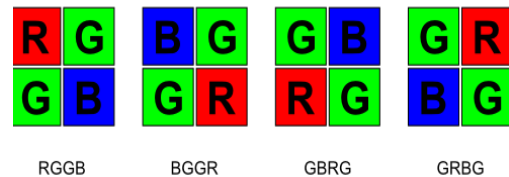


Figure 1. CFA Bayer Pattern.

sample the values can be estimated and correlated with its neighbors [12]. Bilinear interpolation applications by taking an average of four neighboring pixels to obtain interpolation values, multiplication product with bilinear interpolation matrix h_r , h_g , dan h_b . For example bilinear algorithm for red values are unknown at Bayer layer. Pixel $R(x, y)$ that is the red value at x and y position will be interpolated again with CFA algorithm using equation(1) to equation(3).

$$R(2x + 1, 2y) = \frac{R(2x + 1, 2y - 1)}{2} + \frac{R(2x + 1, 2y + 1)}{2} \quad (1)$$

$$R(2x, 2y + 1) = \frac{R(2x - 1, 2y + 1)}{2} + \frac{R(2x + 1, 2y + 1)}{2} \quad (2)$$

$$R(2x, 2y) = \frac{R(2x - 1, 2y - 1)}{4} + \frac{R(2x - 1, 2y + 1)}{4} + \frac{R(2x + 1, 2y - 1)}{4} + \frac{R(2x + 1, 2y + 1)}{4} \quad (3)$$

Furthermore, the calculation of unknown green value at Bayer layer. Pixel $G(x, y)$ that is the green value at x and y position will be interpolated again with CFA algorithm (equation(4)). Green values, which are in even and odd columns and rows, is the average of diagonal nearest neighbor.

$$G(2x, 2y) = \frac{G(2x - 1, 2y)}{4} + \frac{G(2x, 2y - 1)}{4} + \frac{G(2x, 2y + 1)}{4} + \frac{G(2x + 1, 2y)}{4} \quad (4)$$

Finally, for the unknown blue value at Bayer layer. Pixel $B(x, y)$ that is the blue value at x and y position will be interpolated again with CFA algorithm using equation(5) to equation(7).

$$B(2x + 1, 2y) = \frac{B(2x - 1, 2y)}{2} + \frac{B(2x + 1, 2y)}{2} \quad (5)$$

$$B(2x, 2y + 1) = \frac{B(2x, 2y - 1)}{2} + \frac{B(2x, 2y + 1)}{2} \quad (6)$$

$$B(2x, 2y) = \frac{B(2x - 1, 2y - 1)}{4} + \frac{B(2x - 1, 2y + 1)}{4} + \frac{B(2x + 1, 2y - 1)}{4} + \frac{B(2x + 1, 2y + 1)}{4} \quad (7)$$

Wavelet Transformation

Analysis of Wavelet decomposition and reconstruction using approximation coefficients and detail coefficients. Approximation coefficients have high scale and low signal frequency components. Detail coefficients have low scale and high frequency components. Wavelet are formed using a low-pass and high-pass filter. According to Rao and Bopardikar [13] low-pass filter is useful for interpolating and smoothing noise, while the high-pass filter is useful in extracting edges and sharpen image.

Wavelet base comes in a scaling function derived from the dilation equation, as the basis of Wavelet theory. Scaling function equation is expressed by the following equation(8).

$$\phi(x) = \sum_{k=0}^N c_k \phi(2x - k) \quad (8)$$

where $\phi(x)$ is a function of Wavelet dilation equation, c_k is a Wavelet coefficient, k is a positive integer, N is number of elements and x is value of matrix element. Scaling function equation can form a first Wavelet equation or mother Wavelet, namely as given by equation(9).

$$\varphi^0(x) = \sum_{k=0}^{N-1} (-1)^k c_{1-k} \phi(2x - k) \quad (9)$$

where $\varphi^0(x)$ is a scaling function for mother Wavelet, c_k is a Wavelet coefficient, k is a positive integer, N is number of pixel elements, and x is value of matrix element. Mother Wavelet then be formed Wavelet φ^1 , φ^2 and so on. In large-scale wavelet φ is used for macro analysis, while small-scale wavelet Ψ used for micro analysis on the signal.

Forensic Digital Image Manipulation Scheme

The CFA interpolation scheme aims to make reconstruction once again in the input image using

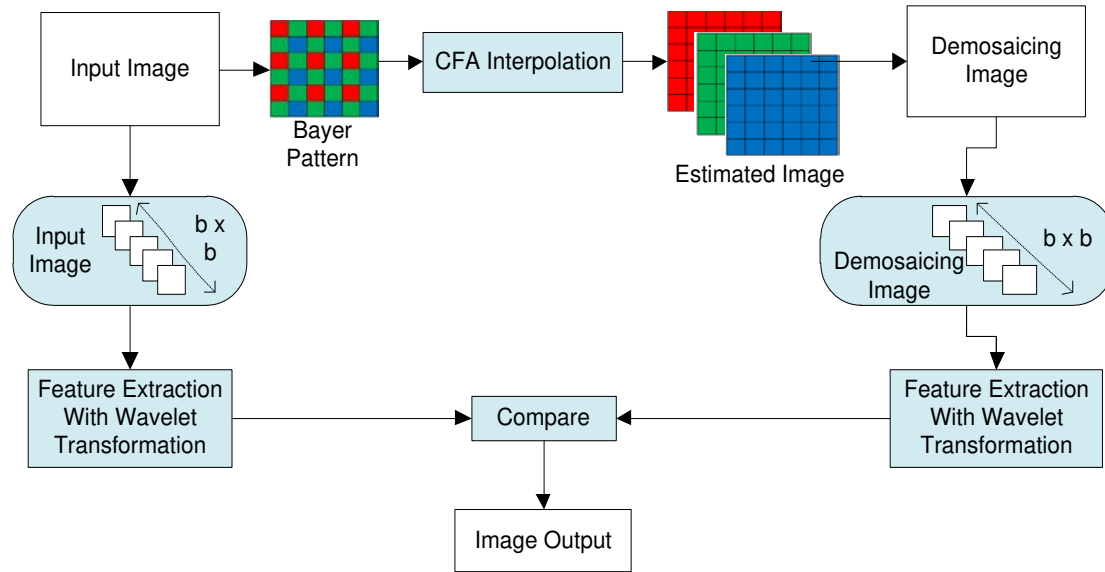


Figure 2. Digital image forgery detection scheme.

Bayer pattern which is considered as information from image of CFA sensor result on digital cameras [14]. Each pixel values in the image interpolation correlated with the weight of pixel amount from nearest neighbors. Furthermore, image results will be evaluated by PSNR. Image interpolation results which have the largest PSNR value will be considered as original parameters used in image formation, when the object is taken on a digital camera.

Bayer layer pattern lead CFA color filter arranged in a periodic pattern and has correlation that also periodic. Interpolation calculation produces estimated values for the three RGB channels. CFA interpolation scheme using bilinear algorithm and Wavelet transformation can be seen in Figure 2. For a manipulated image, the spliced part comes from the different images, which undergoes different demosaicking algorithm. Furthermore, the spliced part, to fit into the original image, is often rotated, resized to fit the target location, which would makes the interpolation relationship different from original one. So, by checking the error rate on each pixel, we can determine the spliced parts.

3. Results and Analysis

Image splicing is a merger of one or more digital image into a new image that is visually as the original image. The whole false images in this study manipulated with image editing software Adobe Photoshop CS and Macromedia Fireworks. The evaluation calculation of this digital image forgery detection algorithm performance using Peak Signal to Noise Ratio (PSNR). PSNR calculation

to measure the quality of input image and quality of reconstruction image from CFA interpolation result.

Digital image data in this research using primary and secondary image data. The input image has different splicing manipulation, whose forged parts come from the same target images; in splicing forgery, forged part comes from a different source image. For the primary image data retrieved from the dataset released by the University of Enlargen Denmark in Image Manipulation Dataset. This dataset was taken to compare image forgery with merger of indoor and outdoor images, and merger images from multiple different brands of digital cameras such as Nikon, Canon, and Kodak. Furthermore for the secondary data taken from private collections with digital camera, Nokia phone camera, and Internet down-loads. All digital camera images stored in JPG format. Selection of mobile phone digital camera based on reality that developed in community, which is the high usage of digital cameras, especially on the phone rather than using a regular digital camera. This can increase the chances of digital image manipulation performed by general public. Input image from Internet downloads as a system testing for image authenticity that circulate in the community that can be downloaded for free on the Internet.

The experiment were performed in the MATLAB environment version 7.10.0.499 (R2010a) on a PC equipped with a Intel Core i3 M350 2.27 GHz CPU with 3 GB of RAM, and running the Windows 7 Ultimate operating system.

Evaluation test by comparing the input image with the demosaicing image from four Bayer

TABLE 1
PSNR VALUE OF PRIMARY IMAGE DATASET INTERPOLATION RESULTS WITH 4 CFA PATTERN AND AUTHENTICITY DETECTION RESULTS.

No.	Input Image	CFA Bayer PSNR (dB)				Time (s)	Detection Image	Ground Truth
		Pattern 1	Pattern 2	Pattern 3	Pattern 4			
1	Ocanonxt_kodakdcs330_sub_05.tif	40.59	40.62	40.52	40.33	68.071877	Fake	Fake
2	Ocanonxt_kodakdcs330_sub_10.tif	40.82	40.89	40.81	40.84	78.447702	Fake	Fake
3	Ocanonxt_kodakdcs330_sub_14.tif	39.59	39.55	39.37	39.67	69.275378	Fake	Fake
4	Ocanonxt_kodakdcs330_sub_16.tif	41.03	41.39	41.31	40.87	69.285874	Fake	Fake
5	Ocanonxt_kodakdcs330_sub_17.tif	39.48	39.31	39.72	39.31	68.246909	Fake	Fake
6	Ocanonxt_kodakdcs330_sub_21.tif	41.03	41.28	41.20	40.93	69.804334	Fake	Fake
7	Ocanonxt_kodakdcs330_sub_27.tif	37.34	37.28	37.28	37.29	67.710555	Fake	Fake
8	Ocanonxt_kodakdcs330_sub_28.tif	35.53	35.50	35.56	35.54	68.495571	Fake	Fake
9	Ocanonxt_kodakdcs330_sub_30.tif	37.09	37.38	37.38	37.11	68.902182	Fake	Fake
10	Ocanonxt_kodakdcs330_sub_25.tif	37.51	37.27	37.31	37.36	67.710497	Fake	Fake
11	Ocanonxt_02_sub_01.tif	44.80	44.76	44.67	44.42	104.94415	Original	Original
12	Ocanonxt_02_sub_08.tif	40.98	41.27	41.11	40.90	105.60424	Original	Original

TABLE 2
PSNR VALUE OF SECONDARY IMAGE DATASET INTERPOLATION RESULTS WITH 4 CFA PATTERN AND AUTHENTICITY DETECTION RESULTS.

No.	Input Image	CFA Bayer PSNR (dB)				Time (s)	Detection Image	Ground Truth Pattern
		Pattern 1	Pattern 2	Pattern 3	Pattern 4			
1	0UNIB_S1.tif	36.15	36.33	36.37	36.11	71.213186	Fake	Fake
2	0UNIB_S4.tif	36.39	36.42	36.45	36.39	97.547486	Fake	Fake
3	OS_IP.tif	38.47	38.38	38.52	38.28	69.743820	Fake	Fake
4	2014-11-10-4390.tif	30.78	30.80	30.81	30.78	64.7343	Fake	Fake
5	OP_IS_1.tif	40.36	40.89	40.42	40.79	71.523089	Fake	Fake
6	IS_OP_1.tif	33.88	33.92	33.92	33.91	74.312988	Fake	Fake
7	IMG_17219338723821.jpeg	31.82	31.99	32.05	31.80	0.299019	Fake	Fake
8	IMG_17243954722362.jpeg	30.48	30.49	30.54	30.52	0.228797	Fake	Fake
9	IMG_17237492692976.jpeg	32.14	32.15	32.16	32.15	0.193201	Fake	Fake
10	2014-11-10-4389.jpg	31.40	31.51	31.46	31.47	0.740270	Fake	Fake
11	2014-12-02-4598.jpg	40.00	40.03	40.75	40.28	0.809416	Original	Original
12	IP_2.tif	40.45	40.42	40.55	40.56	62.685728	Original	Original

pattern. That fourth Bayer pattern is (1) GRBG, (2) GBRG, (3) BGGR, and (4) RGGG. Visual quality measurement using PSNR of interpolation result image to see the differences and changes in pixel intensity values in each color channel. The higher the PSNR values that achieved by one of Bayer pattern at CFA interpolation result image, then that image is closer to the original pattern when shooting from a digital camera. Units used to express the PSNR is decibels (dB).

Image forgery detection process passively carried directly to input image, without knowing the initial information about original image. Comparisons are made to the input image toward CFA interpolation result image with the highest PSNR (see Table 1). Future studies evaluating system using secondary data which image data taken from a private collection with a digital camera, Nokia phone camera, and manipulated image from Internet (see Table 2).

Our method goes further to label the forged region for a sliced image. Since the spliced part

have undergone different demosaicking algorithm from the original image, thus we exclude the spliced parts and approximate the interpolation via the original part. From the results given in Table 1 and Table 2, it seen that this method can be used to detect different image tampering operations with high accuracies.

In our experiments, we apply the proposed method to solve two problems in image forensics: spliced image identification and exposing spliced area. Local image forgery generally distorts image statistics in tampered image region. Therefore, it is expected that tampered image region should yield different CFA demosaicking artifacts as compared to the rest of the image (see Table 3).

The input image is re-interpolated with four candidate CFA pattern aims to identify the CFA pattern of an image. The second pattern and the third pattern give a good PSNR result better than the other pattern. Because of this pattern is the best candidate pattern on an estimation for CFA interpolation pattern of the source digital camera.

TABLE 3
DETECTION IMAGE



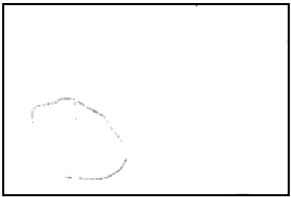


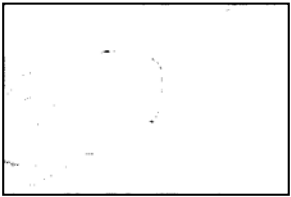


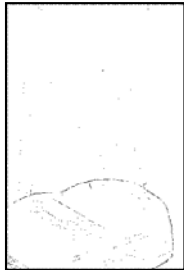
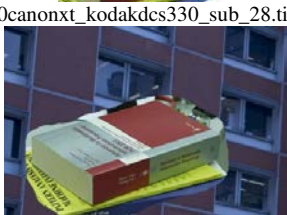




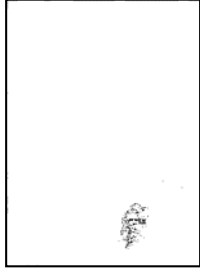


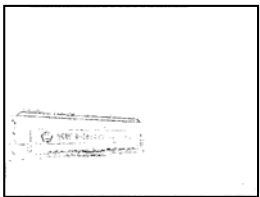


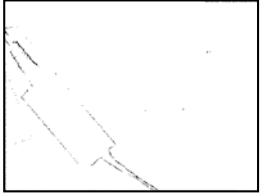
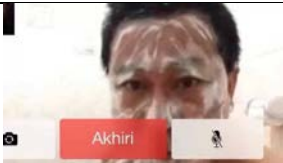

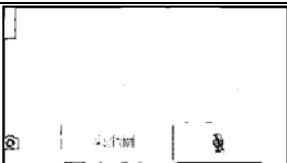


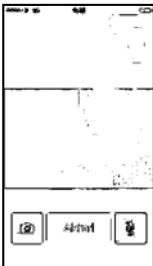








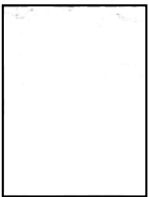





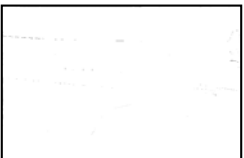
No.	Input Image	Demosaicking Image	Detection Image
1.	 0canonxt_kodakdcs330_sub_05.tif	 CFA Bayer Pattern 2	
2.	 0canonxt_kodakdcs330_sub_14.tif	 CFA Bayer Pattern 4	
3.	 0canonxt_kodakdcs330_sub_28.tif	 CFA Bayer Pattern 3	
4.	 0canonxt_kodakdcs330_sub_25.tif	 CFA Bayer Pattern 1	
5.	 2014-11-10-4390.tif	 CFA Bayer Pattern 2	
6.	 0UNIB_S4.tif	 CFA Bayer Pattern 3	
7.	 OS_IP.tif	 CFA Bayer Pattern 3	

TABLE 3 CONTINUE
DETECTION IMAGE

No.	Input Image	Demoaicking Image	Detection Image
8.	 IMG_17219338723821.jpeg	 CFA Bayer Pattern 3	
9.	 IMG_17237492692976.jpeg	 CFA Bayer Pattern 3	
10	 IS_OP_1.tif	 CFA Bayer Pattern 3	
11	 2014-12-02-4598.jpg	 CFA Bayer Pattern 3	
12	 IP_2.tif	 CFA Bayer Pattern 4	
13	 Ocanonxt_02_sub_01.tif	 CFA Bayer Pattern 1	
14	 Ocanonxt_02_sub_08.tif	 CFA Bayer Pattern 2	

In Table 1 and Table 2 above shows that the system has managed to do an image forensic that precisely estimating the input image as a false image that corresponds to the direct examination data (*ground truth*). PSNR value in interpolation result image for each Bayer pattern showed a significant difference.

4. Conclusion

Based on the experimental results and analytical evaluation of digital image forgery detection method for *image splicing* forgery types using the CFA method and wavelet transform, it can be concluded as follows: 1) CFA method implementation in input image aims to get interpolation image, because in image forgery detection by passive approach there is no initial information of original image. Therefore, the interpolation result image is considered as a benchmark image in forgery detection, because interpolation image is an image that is closest to the original pattern before manipulated. 2) Analysis of interpolation image results obtained by combining CFA interpolation algorithm and wavelet transform has been able to improve the image quality of interpolation results. The higher the PSNR in interpolation image, meaning that the image closer to the original image patterns exist when shooting from a digital camera. PSNR value range for the primary and secondary dataset image is between 30.48 and 41.39 dB with an average of overall PSNR is 36.93 dB. In general, the best CFA Bayer pattern is the second pattern (GBRG) and the third pattern (BGR). 3) CFA interpolation and wavelet algorithm has been able to detect image forgeries with a passive approach. By using primary data from *Image Manipulation Dataset* and secondary data from a private collection and manipulated images from the Internet, the system has been able to estimate the image area that is estimated to have experienced digital manipulation.

Overall, digital image forgery detection method was able to identify false images and mark image area that has been manipulated well. However, this algorithm has a quite large time complexity. Therefore, they need to do further research to develop CFA interpolation with better interpolation image quality and low time complexity. One limitation is that proposed image splicing detection techniques are sensitive to strong JPEG recompression and resizing. Since these type of operations distort the CFA artifacts.

The limitation of the purposed method are sensitive to strong JPEG compression and resizing. Since these type of operations distort CFA artifacts. CFA based image splicing detection may not be successful after these operations.

This topic is still open up the opportunities for further research with a variety of forms and digital image forgery categories, along with post-processing attacks that is done to cover the traces of digital image forgery. In the end will produce the digital image forgery detection method that is more robust, effective, efficient, and in accordance with the development of digital technology.

References

- [1] Harian Rakyat Bengkulu, Kolor Ijo Bikin Heboh, <http://www.harianrakyatbengkulu.com/kolor-ijo-bikin-heboh/>, retrieved February 1, 2014.
- [2] M.H. Olesen, Detecting Photographic Manipulation, <http://www.hollmen.dk>, 2006, retrieved September 8, 2009.
- [3] H. Farid, In Deception: From Ancient Empires to Internet Dating, *Digital Doctoring: Can We Trust Photographs?*, Dartmouth College, USA, 2009.
- [4] E.P. Purwandari, "Deteksi Pemalsuan Citra Digital Berbasis Singular Value Decomposition dan Color Filter Array," Magister Thesis, Computer Science Magister, Computer Science Faculty, University of Indonesia, Indonesia, 2011.
- [5] W. Zhang, J. Cao, Zhu, & P. Wang, "Detecting Photographic Composites using Shadows," *IEEE International Conference on Multimedia and Expo*, pp. 1042–1045, 2009.
- [6] Y.F. Hsu, & S.F. Chang, "Image Splicing Detection using Camera Response Function Consistency and Automatic Segmentation," *In Multimedia and Expo, IEEE International Conference on*. IEEE, 2007, pp. 28–31, 2007.
- [7] W. Chen, Y.Q. Shi, & W. Su, "Image splicing detection using 2-d phase congruency and statistical moments of characteristic function," *Security, Steganography and Watermarking of Multimedia Contents IX, Proceeding. of SPIE*, 2007.
- [8] Y.Q. Shi, C. Chen, & W. Chen, "A natural image model approach to splicing detection," *In MM & Sec '07: Proceedings of the 9th workshop on Multimedia & security*, pp. 51–62, 2007.
- [9] A. E. Dirik, S. Bayram, H. T. Sencar, & N. Memon, "New features to identify computer generated images," *In IEEE International Conference on Image Processing, ICIP '07*, vol. 4, pp. 433–436, 2007.
- [10] A. C. Gallagher & T. Chen, "Image Authentication by Detecting Traces of Demosaicing," *In Proc. CVPR WVU Workshop, ia and Expo*, pp. 1042–1045, 2008.

- [11] S. Bayram, H.T. Sencar, & N. Memon, "Classification of Digital Camera Models Based on Demosaicking Artifacts," *Digital Investigation Elsevier*, vol. 5, pp. 49, 2008.
- [12] R.C. Gonzalez, & P. Wintz, "*Digital Image Processing*," Prentice Hall, 2002.
- [13] M. Rao, & S. Bopardikar, *Wavelet Transform: Introduction to Theory and Applications*, Massachusetts, Addison Wesley Longman, Inc, 1998.
- [14] B.K. Gunturk, J. Glotzbach, Y. Atunbasak, R.W. Schafer, & R.M. Mersereau, "Demosaicking: Color Filter Array Interpolation," *IEEE Signal Processing Magazine*, pp 44-54. 2005.