International Journal of Digital Crime and Forensics
Volume 11 • Issue 2 • April-June 2019

Digital Image Forensics Based on CFA Interpolation Feature and Gaussian Mixture Model

Xinyi Wang, Beijing University of Posts and Telecommunications, Beijing, China
Shaozhang Niu, Beijing University of Posts and Telecommunications, Beijing, China
Jiwei Zhang, Beijing University of Posts and Telecommunications, Beijing, China

ABSTRACT

According to the characteristics of the color filter array interpolation in a camera, an image splicing forgery detection algorithm based on bi-cubic interpolation and Gaussian mixture model is proposed. The authors make the assumption that the image is acquired using a color filter array, and that tampering removes the artifacts due to a demosaicing algorithm. This article extracts the image features based on the variance of the prediction error and create image feature likelihood map to detect and locate the image tampered areas. The experimental results show that the proposed method can detect and locate the splicing tampering areas precisely. Compared with bi-linear interpolation, this method can reduce the prediction error and improve the detection accuracy.

KEYWORDS

Bi-Cubic Interpolation, CFA Interpolation, Gaussian Mixture Model, Splicing Forgery Detection

1. INTRODUCTION

In recent years, with the popularity of smart phones and high-performance digital acquisition equipment widely used, digital images are becoming more and more common. At the same time, the image editing tool can easily modify the image content. So this prompted us to study the authenticity of the image recognition technology. For example, image splicing is commonly used as a method of tampering with two or more images and it is common in image tampering types.

Considering in previous papers, the color filter array (CFA) demosaicing algorithm can be divided into two categories as fingerprints to be analyzed, i) an algorithm designed to estimate the parameters of the color interpolation algorithm, and ii) an algorithm designed to evaluate the presence/absence of a demosaicing trace. Given that the second category focuses on forgery detection (inconsistency in CFA interpolation reveals the existence of forgery regions), the algorithms in the first category are mainly used to classify different source cameras, but sometimes they can also be used to detect tampering.

The color filter array interpolation exists in most cameras, and tampering operations often cause interpolation operations, which makes the study based on the interpolation of image blind evidence technology possible. Popescu (Popescu & Farid, 2005) expounded the main CFA interpolation algorithm, and for the linear interpolation model, the interpolation coefficient was calculated by using the Expectation Maximization algorithm, and the Fourier transform of the probability map was used to further judge whether the image experienced over interpolation operation. Gallagher (Gallagher, 2005)

DOI: 10.4018/IJDCF.2019040101

obtained the second order difference of the image and used the periodic characteristic to detect the image interpolation. The algorithm is limited to bilinear interpolation. Wang Bo (Wang, Kong, You, & Fu, 2009) used the covariance matrix to successfully detect the color filter array interpolation. The above three methods can only detect non-adaptive algorithms. For the adaptive interpolation algorithm, Bayram (Bayram, Sencar, & Memon, 2006) used the periodicity between pixels introduced by CFA interpolation as a classification feature. Peng (Peng, Zeng, Lin, & Kang, 2015) found that irregular sampling and interpolation operations resulted in local linear correlation changes and proposed an algorithm that could effectively detect resampling anti-evidence based on autocorrelation coefficients. Li (Li, Xue, Wang, & Tian, 2015) described the local correlation of the CFA interpolation pattern by establishing a Gaussian model and calculated the posterior probability model of the CFA interpolation and then tampering. In summary, there are many academic achievements in blind forensics of slicing images, especially based on image interpolation. However, many algorithms have some limitations, for example, they can't automatically locate and detect tampered areas, and their accuracy is not high.

This paper is based on the continuity principle that the splicing operation destroys the internal characteristics of the image. It is necessary to interpolate the given image to predicted or estimate its original image. In order to reduce the prediction error, improve the detection accuracy, the image is predicted by bi-cubic interpolation, and then the image feature is extracted based on the variance of the prediction error. Gaussian mixture modeling (GMM) is carried out on the image features of different positions, and the parameters in the model are estimated by EM algorithm. Thereby the tampered area can be detected and located.

The rest of this paper is organized as follows: Section 2 offers an overview of CFA interpolation and Gaussian mixture model. Section 3 gives the proposed approach in detail, while experimental results and conclusion are given in Section 4 and Section 5, respectively.

2. BACKGROUND OF CFA AND GMM

This section gives a brief introduction to the relevant knowledge that can help to understand the analysis method based on CFA interpolation and Gaussian mixture model.

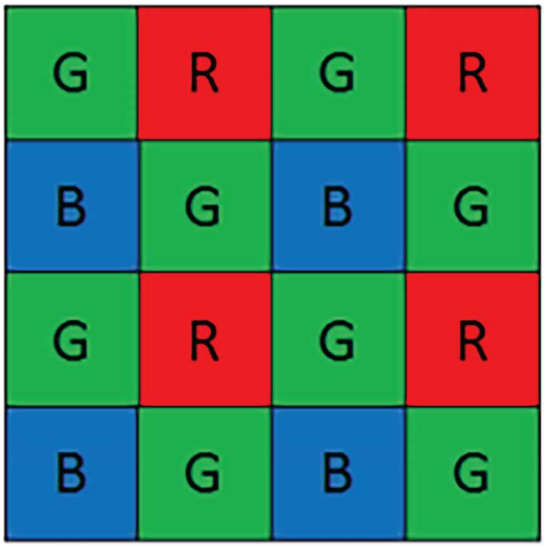
2.1. CFA Interpolation

A digital color image consists of three channels containing samples from different bands of the color spectrum: red, green, and blue. Considering the cost and the system volume of digital cameras, most of them use a single charge-coupled (CCD) sensor arrays as sensor components and capture color images using a color filter array (CFA).

Color filter array is usually in the form of a board, because the color filter arrangement and the proportion are different, the structure of CFA can be divided into many kinds. Bayer CFA (Bayer, 1976) is one of the most common arrays, as indicated in Figure 1, where green (G) values are sampled in a quincunx lattice while red (R) and blue (B) values are in two separate rectangular lattices. The simplest approach to demosaicing is bilinear interpolation (Longere, Zhang, & Delahunt, 2002), in which the three color planes are independently interpolated using symmetric bilinear interpolation from the nearest neighbors of the same color. If Bayer CFA is covered on a sensor surface, only one color in red, green or blue can be obtained at a certain pixel (Gunturk, 2005).

For the area where the CFA is not interpolated in the image, the likelihood that a pixel value is associated with the surrounding pixel value is small. For the area that have been subjected to CFA interpolation, there is a large correlation between a pixel value in the region and the surrounding pixel value, and the tampering operation causes the correlation between the pixels to be corrupted (Hsu, & Chang, 2006; Luo, Liao, Zheng, & Deng, 2016; Swaminathan, Wu, & Liu, 2008). For this reason, the inconsistency in tampered regions can be utilized as clues to detect the tampered areas.

Figure 1. The Bayer's filter mosaic



2.2. Gaussian Mixture Model

The Gaussian mixture model (GMM) is a simple linear superposition model of Gaussian distribution. Compared with the single Gaussian model, the Gaussian mixture model is designed to provide a richer classification for the density model. Using a certain number of Gaussian distributions and adjusting their mean, covariance, and linear combination coefficients, then the majority of the continuous density can be approximated to any precision.

The N-dimensional vector $y_1, y_2 \ldots y_n$ of the K Gaussian models is assumed to be subordinate to the independent distribution. The probability density function is shown in Equation (1). This Gaussian model is called the Gaussian mixture model. Here, E, ¼ Σ are the mixed parameter, mean and the covariance matrix:

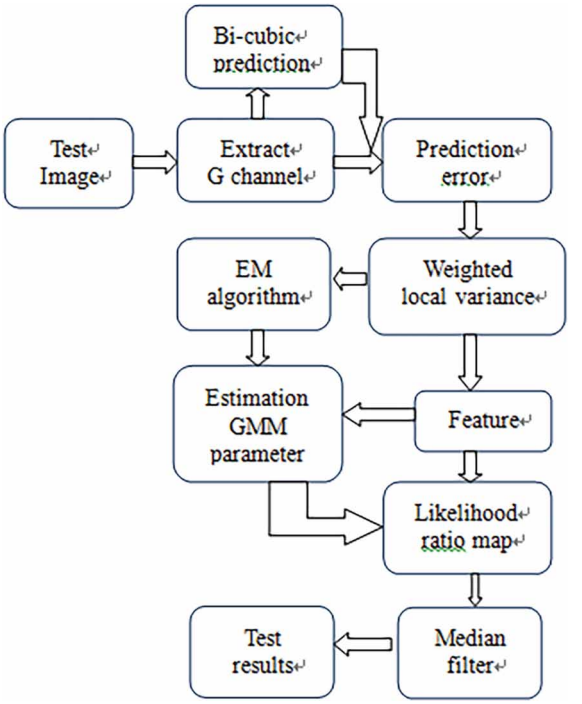
$$P(y) = \sum_{k=1}^{K} \omega_k N\left(y_K | \mu_K, \Sigma_K\right) \tag{1}$$

3. METHODOLOGY

In this section, the process of our method is: First, extract the Green channel to predict the original image. Second, get the original image estimation by the given image. Then the image pixel value of the image at different positions is modeled by Gaussian mixture, and the EM algorithm (Redner, & Walker, 1984) is used to estimate the parameters in the model. Finally, by establishing the log likelihood ratio of the image feature, we can get the tamper detection map. The framework of the proposed method is shown in Figure 2.

The method can be divided into the following three main processes.

Figure 2. Framework of the proposed method



3.1. Feature Extraction Based on Prediction Error

Take the pixel values at x_0 in the Bayer CFA image for example, which can be seen in Figure 3(b), the bi-cubic interpolation is used, and the pixel value at x_P is interpolated as:

$$\boldsymbol{x}_P = \frac{1}{4}\begin{pmatrix} \boldsymbol{x}_1 - 9\boldsymbol{x}_2 - 9\boldsymbol{x}_3 - 9\boldsymbol{x}_4 + 81\boldsymbol{x}_5 - 9\boldsymbol{x}_6 + \boldsymbol{x}_7 + 81\boldsymbol{x}_8 \\ +81\boldsymbol{x}_9 + \boldsymbol{x}_{10} - 9\boldsymbol{x}_{11} + 81\boldsymbol{x}_{12} - 9\boldsymbol{x}_{13} - 9\boldsymbol{x}_{14} - 9\boldsymbol{x}_{15} + \boldsymbol{x}_{16} \end{pmatrix} \tag{2}$$

The prediction error e(x, y) of G channel is:

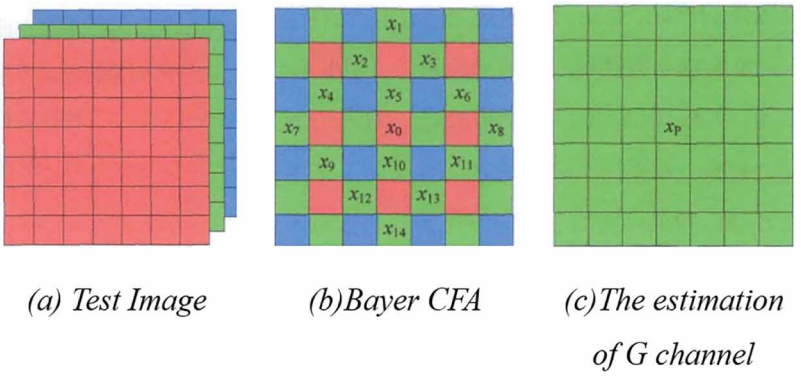
$$e\left(x,y\right) = G\left(x,y\right) - G_p\left(x,y\right) = G\left(x,y\right) - \sum_{u,v\neq 0} h_P\left(u,v\right) G\left(x+u, y+v\right) \tag{3}$$

where $\mathrm{G}\left(x,y\right)$ represents the pixel value in the G channel of the image need to be detected, $\mathrm{G}_p\left(x,y\right)$ represents the pixel value in the predicted G channel (Park, Song, & Kang, 2017), h_p represents the predicted kernel.

In order to further analyze the feature of the prediction error, we calculate the local weighted variance and mean of the prediction error. According to the Bayer model, the prediction error obtained is divided into two categories. The prediction error of the device acquisition pixel $\mathrm{e}_A\left(x,y\right)$ and the prediction error of the pixel from the CFA interpolation $\mathrm{e}_I\left(x,y\right)$.

We can extract the feature F of the image need to be detected by the following formulas:

Figure 3. The prediction of G channel



$$G_{M_A}\left(k,l\right)=\left[\prod_{i,j\in b_A}\sigma_A^2\left(i,j\right)\right]^{1/\left|b_A\right|} \tag{4}$$

$$F\left(k,l\right)=\ln\frac{G_{M_A}\left(k,l\right)}{G_{M_I}\left(k,l\right)} \tag{5}$$

$\mathrm{G}_{M_A},\mathrm{G}_{M_I}$ are the geometric mean of the image block b_A at the device acquisition and the image block b_L at the CFA interpolation, respectively.

3.2. GMM Based on Tampered and No-Tampered Areas

The area in the image can be divided into two types, one with CFA interpolation M_1 (no-tampered area) and the other without CFA interpolation M_2 (tampered area).

If the image need to be detected has been tampered, the effect of CFA interpolation on the image at the tampered area will be reduced, where both M_1 and M_2 are present. Therefore, it can be assumed that the feature F obeys the mixed Gaussian distribution, and the features of the different areas conform to the Gaussian mixture model. The features conforming to M_1 and M_2 are modeled separately, which are shown as:

$$P\left\{F(k,l|M_1)\right\}=N\left(\mu_1,\sigma_1^2\right) \tag{6}$$

$$P\left\{F(k,l|M_2)\right\}=N\left(\mu_2,\sigma_2^2\right) \tag{7}$$

where $\acute{\mathrm{E}}_1$ and $\acute{\mathrm{E}}_2$ are the mixing coefficient, and $\acute{\mathrm{E}}_1+\acute{\mathrm{E}}_2=1$. The distribution of the image feature is $\acute{\mathrm{E}}_1\cdot\mathrm{N}\left(¼_1,\tilde{\mathrm{A}}_1^2\right)+\acute{\mathrm{E}}_2\cdot\mathrm{N}\left(¼_2,\tilde{\mathrm{A}}_2^2\right)$. We employ the Expectation Maximization (EM) algorithm. It is

a standard iterative algorithm that estimates the mean and the variance of the component distributions by maximizing the expected value of a complete log-likelihood function with respect to the distribution parameters. In our case, the EM algorithm is used to estimate only $¼_1$, σ_1 and σ_2, since we assume $¼_2 = 0$.

3.3. Create Image Feature Likelihood Map

In order to further detect and locate the image tampered area, it is necessary to obtain the probability that the area belongs to the no-tampered area and tampered area separately, that is $\mathrm{P}\left\{\mathrm{M}_1|\mathrm{F}\left(\mathrm{k},\mathrm{l}\right)\right\}$ and $\mathrm{P}\left\{\mathrm{M}_2|\mathrm{F}\left(\mathrm{k},\mathrm{l}\right)\right\}$. According to the Bayesian formula, $\mathrm{P}\left\{\mathrm{M}_1|\mathrm{F}\left(\mathrm{k},\mathrm{l}\right)\right\}$ can be obtained as:

$$P\left\{M_1|F\left(k,l\right)\right\} = \frac{P\left(M_1\right)P\left\{F(k,l|M_1)\right\}}{P\left(M_1\right)P\left\{F(k,l|M_1)\right\} + P\left(M_2\right)P\left\{F(k,l|M_2)\right\}} \tag{8}$$

$$P\left\{M_1|F\left(k,l\right)\right\} = \frac{1}{1 + \dfrac{P\left(M_2\right)P\left\{F(k,l|M_2)\right\}}{P\left(M_1\right)P\left\{F(k,l|M_1)\right\}}} \tag{9}$$

Define the likelihood ratio of the image feature F as:

$$lnl\left(F\left(k,l\right)\right) = ln\frac{P\left\{F(k,l|M_2)\right\}}{P\left\{F(k,l|M_1)\right\}} = ln\sigma_1 - \ln\sigma_2 - 0.5\left[\frac{\left(x-\mu_1\right)^2}{\sigma_2^2} - \frac{\left(x-\mu_1\right)^2}{\sigma_1^2}\right] \tag{10}$$

In order to further improve the positioning performance, we noticed that in a real fake image, the tampered area is usually a connected area due to the semant content of the image. By applying a simple low-pass spatial filter such as an averaging filter or a median filter on the map, these connected areas can be distinguished. For better numerical stability, we apply this filter to the logarithm of the likelihood map. In this paper, the cumulative operation based on the logarithmic likelihood ratio is calculated and blurred with a 7x7 median filtered to remove the noise in the detection map to obtain the likelihood image of the image to be detected and finally to complete the tamper detection.

4. EXPERIMENTS

Image splicing operations include copy-move (Amerini, Ballan, Caldelli, Bimbo, Tongo, & Serra, 2013) and copy-splice (Pun, Liu, & Yuan, 2016) two tamper operations. In this section, the same images in Ferraras' (Ferrara, Bianchi, Rosa, & Piva, 2012) are employed to test the performance of the proposed algorithm. The original image database is composed of Canon EOS 450D, Nikon D50, Nikon D90 and Nikon D7000. All cameras are equipped with a Bayer CFA. Each image was cropped to 356 × 356 pixels, maintaining the original Bayer pattern, which is assumed to be known. We will refer to such a dataset as the original dataset.

In this paper, the experiment is conducted in Matlab R2015a, the operating environment is Intel (R) Core (TM) CPU@ 3.40GHz i7-4770, 16GB memory PC machine.

4.1. Threshold Determination

When the GM algorithm is used to estimate the GMM parameters, the initial values of the mixed coefficients $\acute{E}_1$, $\acute{E}_2$ are set to 0.5, and the initial value of $¼_1$ is the mean of the feature. The initial values of the variance $\tilde{A}_1^2$ and $\tilde{A}_2^2$ are the variance of the feature. Set the EM algorithm to the end of the iteration conditions: the maximum number of iterations is 400 times, the maximum allowable parameter error is 0.001.

4.2. Copy-Paste Forgery Detection

Ferrara et al.'s database contains different types of tamper images, which include a portion of the copy-move image. Based on the detection algorithm proposed in this paper, the copy-move image is detected. The experimental results show that the algorithm proposed in this paper can effectively realize the detection of the copy-move image and realize the location of the tampering area. Some of the test results are listed here.

Figure 4 is an example of a copy-move forgery in an image with CFA artifacts. The resulting image is saved in TIFF format, and original image acquired by the Nikon D90 camera. (a)' and (b)' show histogram histograms based on image sizes of 2×2 and 6×6. It can be seen from the histogram of the feature that the block size will affect the extracted features. The Smaller, the more detailed the extracted features we can get, the larger the block size, the less the extracted features we can get. (a)'' and (b)'' show the block size of 2×2 and 6×6 tamper detection results, the test results can be seen, the smaller the size of the block, the more accurate positioning, but can't better resist the noise on the test results of the interference; The larger the block size, the lower the positioning accuracy, but can reduce the impact of noise.

According to the experimental results, the algorithm based on the proposed method can realize the tampering of the replicated image and the detection precision is high, and the automatic positioning of the copy area can be realized.

4.3. Copy-Splice Forgery Detection

The splicing image in the database is made up of the real images obtained by any two of the cameras described above. The image in this image database only undergoes a single splicing operation, so it can be used for testing tests for splicing operations. Some of the test results are listed here.

In Figure 5, we show a forgery in which a processed content (statue) is pasted on an image with CFA artifacts. Figure 6 is spliced by multiple images.

In order to further detect all the tampered images in the image database, the accuracy rate P_A is used to measure the results of the tamper detection. The accuracy is calculated as:

$$P_A = \frac{N_T}{N_T + N_F} \tag{11}$$

where N_T indicates the number of tamper images successfully detected, and N_F indicates the number of tampering images that are missing. Table 1 shows the test results of splicing image forensics.

The above tamper detection experiments show that the proposed algorithm in this chapter can effectively capture the difference between the measured image and the estimated original image, so that the accuracy of splicing detection can reach 2x2 pixel level and over 84%, indicating that the proposed algorithm is more effective.

From Table 2, we can see the proposed algorithm is more accurate than the Ferraras' method in (Ferrara, Bianchi, Rosa, & Piva, 2012), and when the block size is larger, more splicing images are detected. Due to the presence of uniform or very sharp regions, automatic detection may give a remarkable false positive rate.

Figure 4. The example of copy-move forgery detection

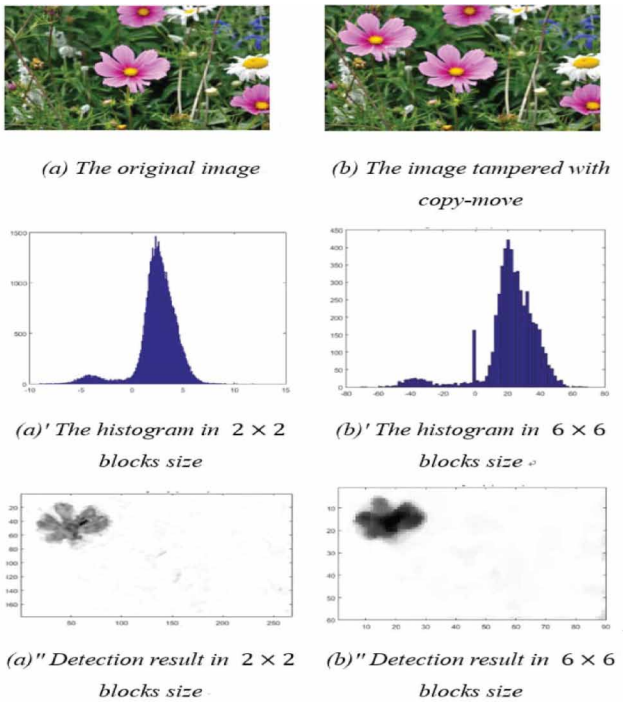


Figure 5. The example of copy-splice forgery detection

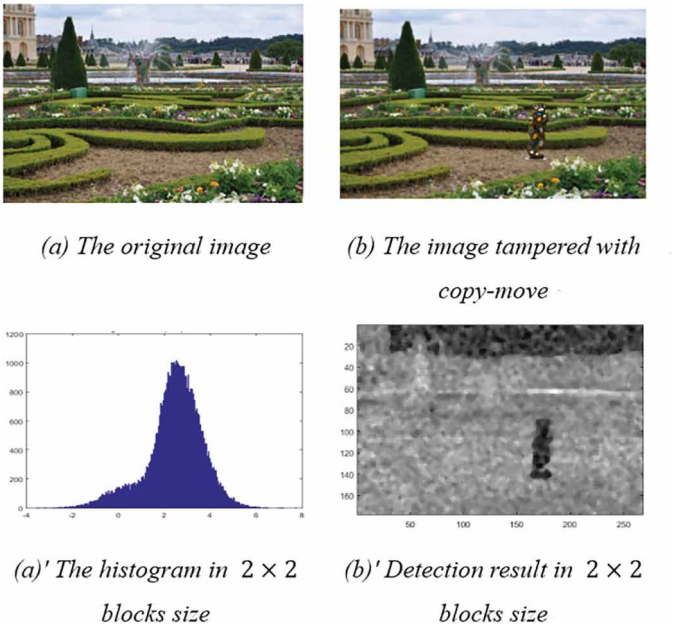


Figure 6. The example of multiple copy-splice forgery detection

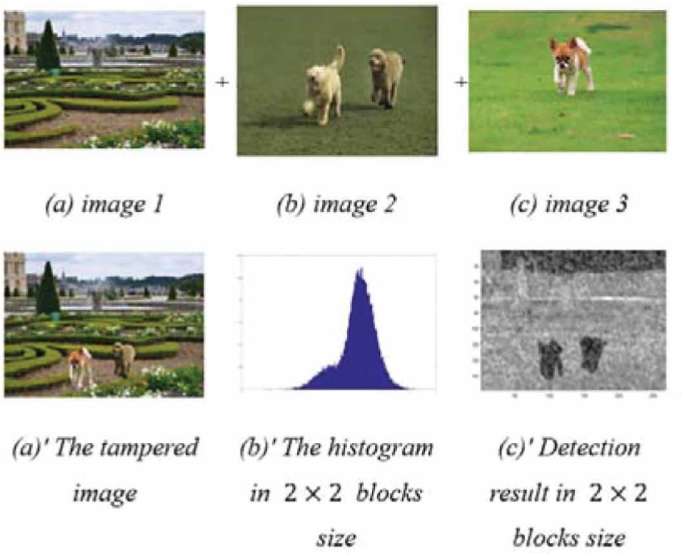


Table 1. The test results of splicing image forensics (block size is 2×2)

Source of Splicing Image	Image Number $(N_T + N_F)$	Successful Number N_T	Precision(%) P_A
Canon EOS 450D+ Nikon D50	30	25	83.33%
Nikon D50+Nikon D90	30	26	86.67%
Canon EOS 450D+ Nikon D7000	30	25	83.33%
Total	90	76	84.44%

Table 2. Comparison results for splicing image forensics

Ferraras' Method		Our Method	
2×2	4×4	2×2	4×4
82.22%	86.67%	84.44%	88.89%

5. CONCLUSION

In this paper, a new method for blind detection of image splicing is proposed, which combines bi-cubic interpolation and Gaussian mixture model to detect and locate splicing forgery. Compared with existing work, this method can reduce the prediction error and improve the detection accuracy. But the detection effect is not ideal after adding noise or jpeg compression. Therefore, we will focus on this issue in future.

ACKNOWLEDGMENT

This work was supported by National Natural Science Foundation of China (No. 61370195, U1536121).

REFERENCES

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. D., Tongo, L. D., & Serra, G. (2013). Copy-move forgery detection and localization by means of robust clustering with j-linkage. *Signal Processing Image Communication*, *28*(6), 659–669. doi:10.1016/j.image.2013.03.006

Bayer, B. E. (1976). *Color imaging array*.

Bayram, S., Sencar, H., & Memon, N. (2006). *Identifying Digital Cameras Using CFA Interpolation. Advances in Digital Forensics II*. Springer New York.

Ferrara, P., Bianchi, T., Rosa, A. D., & Piva, A. (2012). Image forgery localization via fine-grained analysis of cfa artifacts. *IEEE Transactions on Information Forensics and Security*, *7*(5), 1566–1577. doi:10.1109/TIFS.2012.2202227

Gallagher, A. C. (2005). Detection of Linear and Cubic Interpolation in JPEG Compressed Images. In *Proceedings. the, Canadian Conference on Computer and Robot Vision 2005* (pp. 65-72). IEEE.

Gunturk, B. K., Glotzbach, J., Altunbasak, Y., Schafer, R. W., & Mersereau, R. M. (2005). Demosaicking: Color filter array interpolation. *IEEE Signal Processing Magazine*, *22*(1), 44–54. doi:10.1109/MSP.2005.1407714

Hsu, Y., & Chang, S. (2006). Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency. In *IEEE International Conference on Multimedia and Expo* (pp. 549-552). IEEE. doi:10.1109/ICME.2006.262447

Li, L., Xue, J., Wang, X., & Tian, L. (2015). A robust approach to detect digital forgeries by exploring correlation patterns. *Pattern Analysis & Applications*, *18*(2), 351–365. doi:10.1007/s10044-013-0319-9

Longere, P., Zhang, X., Delahunt, P. B., & Brainard, D. H. (2002). Perceptual assessment of demosaicing algorithm performance. *Proceedings of the IEEE*, *90*(1), 123–132. doi:10.1109/5.982410

Luo Haiyan, Liao, F., Zheng, W., & Deng, Y. (2016). An ACO algorithm for remote sensing image classification considering correlation among adjacent pixels. *Journal of Geomatics.*

Park, C., Song, K., & Kang, M. (2017). G-channel restoration for RWB CFA with double-exposed w channel. *Sensors (Basel)*, *17*(2), 293. doi:10.3390/s17020293 PMID:28165425

Peng, A., Zeng, H., Lin, X., & Kang, X. (2015). Countering anti-forensics of image resampling. In *IEEE International Conference on Image Processing* (pp. 3595-3599). IEEE.

Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, *53*(10), 3948–3959. doi:10.1109/TSP.2005.855406

Pun, C. M., Liu, B., & Yuan, X. C. (2016). *Multi-scale noise estimation for image splicing forgery detection*. Academic Press, Inc.

Redner, R. A., & Walker, H. F. (1984). Mixture densities, maximum likelihood and the EM algorithm. *SIAM Review*, *26*(2), 195–239. doi:10.1137/1026034

Swaminathan, A., Wu, M., & Liu, K. J. R. (2008). Digital image forensics via intrinsic fingerprints. *IEEE Transactions on Information Forensics and Security*, *3*(1), 101–117. doi:10.1109/TIFS.2007.916010

Wang, B., Kong, X. W., You, X. G., & Fu, H. Y. (2009). Blind cfa interpolation detection based on covariance matrix. *Dianzi Yu Xinxi Xuebao*, *31*(5), 1175–1179.

Xinyi Wang was born in 1991, and is pursuing a Ph.D. degree at the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include information security and digital image forensics.

Shaozhang Niu was born in 1963, currently is a professor at the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include cloud computing, steganography and digital forensics.

Jiwei Zhang was born in 1989, is currently a professor at the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include information security and digital forensics.