Chinese Journal of Electronics
Vol.18, No.3, July 2009

Exposing Copy-Paste-Blur Forgeries Based on Color Coherence*

WANG Bo[1], KONG Xiangwei[1,2], Elisa Bertino[2] and FU Haiyan[1]

(1.*Department of Electronic and Information Engineering, Dalian University of Technology, Dalian 116023, China*)

(2.*CERIAS and Computer Science Department, Purdue University, West Lafayette, Indiana, 47907-2067, USA*)

Abstract — Exposing digital image forgeries is a major challenge for photography authentication and forensics investigation, which aims at proving the authenticity of digital photos. In this paper, we introduce a digital image forensics approach based on color coherence to exposing copy-paste-blur forgeries. We first discuss the inherent color coherence introduced by imaging pipeline, and then obtain several statistical features from the coherence characterization. Using the SVM classifier, we reveal traces of copy-paste-blur tampering in photographic forgeries. Experimental results indicate that the proposed method can effectively expose the copy-paste-blur forgeries and localize the tampered regions with high accuracy.

Key words — Digital image forensics, Photographic forgery, Color coherence, Copy-paste-blur tampering, Feature extraction.

I. Introduction

Digital camera is an efficient and convenient tool to record beautiful views and important events in our lives. The low cost of digital cameras, combined with the availability on Internet of free software for image processing such as Adobe Photoshop, leads to a huge increase in digital image forgeries. The forgeries may negatively impact the perception of news correctness by the public and the trust on scientific discoveries. Even though a suitable solution to such a problem is not only based on technology, an important technical problem that has to be addressed as part of such solution is how to detect digital image forgeries without embedding advance information in images.

Digital image forensics provides tools and methodologies that is used to verify the authenticity and integrity of an image. Considering the scenario, the forensic analysts have no access to the cameras and software tools, which are used for obtaining forgeries, while only some suspicious photographic samples are available. A. Swaminathan called this case completely non-intrusive forensics[1]. To automatically detect duplicated regions in a digital image, an efficient approach is proposed by A.C. Popescu[2] and J. Fridrich[3], which computed the correlations of small fixed-size image blocks. However, these methods only focus on the detection of copy-move forgeries. A more general model of composite pictures is presented in Ref.[4]. The authors extend an effective technique[6] designed for detection of human speech splicing based on bicoherence to image splicing[5]. In recent years, J. Fridrich described a concept called digital "bullet scratches"[7], which means that different digital cameras have unique pattern noise resulting from imperfection of CCD/CMOS sensor. We can establish the pattern noises as a reference, and detect forgeries by determining the absence of the unique one for each individual camera using a correlation detector[8]. However, if the photograph is captured by an unknown camera out of the pattern noise reference, it usually leads to a false alarm.

In this paper, we discuss the inherent color coherence in authentic photographs, and introduce an effective approach to expose copy-paste-blur forgeries by using five features from color coherence characterization. The rest of this paper is organized as follows. We begin with discussing the coherence introduced by the imaging pipeline in Section II. In Section III, the features extracted for detecting copy-paste-blur forgeries are described. We provide the details of the experiments and relevant results in Section IV. Furthermore, a discussion of the effectiveness and reliability of our approach is presented. The paper is summarized in Section V.

II. Color Coherence Introduced by Imaging Pipeline

Most consumer digital cameras use a single sensor to capture a colorful image. The basic structure of imaging pipeline[9] of a typical consumer digital camera is illustrated in Fig.1.

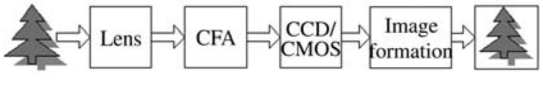


Fig. 1. Block diagram for image acquisition of a digital camera

Considering the cost, the consumer cameras usually use a Color filter array (CFA) and a single sensor to obtain only one

*Manuscript Received July 2008; Accepted Oct. 2008. This work is supported by the National High Technology Research and Development Program of China (863 Program) (No.2008AA01Z418) and the National Natural Science Foundation of China (No.60572111).

color component in a pixel. Fig.2 illustrates the most popular CFA, Bayer CFA. Consequently, through the lens, CFA and CCD/CMOS sensor, a mosaiced image has been captured. To obtain the RGB color image, the two missing colors are interpolated using the sampled pixel values. After the RGB image is generated, the formation processing is carried on and the output image is stored in user-selected image format[10].

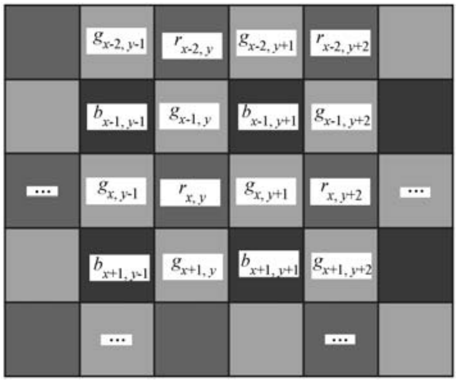


Fig. 2. A portion obtained from a Bayer CFA

No matter which algorithm is adopted, the CFA interpolation introduces specific correlations between the samples[11]. For example, the missing green and blue components at red CFA sampling positions in Fig.2 are given by Eqs.(1–3) using bilinear interpolation:

$$R_{x,y} = r_{x,y} \tag{1}$$

$$G_{x,y} = (g_{x-1,y} + g_{x,y-1} + g_{x+1,y} + g_{x,y+1})/4 \tag{2}$$

$$B_{x,y} = (b_{x-1,y-1} + b_{x-1,y+1} + b_{x+1,y-1} + b_{x+1,y+1})/4 \tag{3}$$

Lossy compression in image formation is another reason of color coherence. Cr and Cb used in JPEG are downsampled because of the relative non-sensitivity of human eyes to chrominance components. Besides, in order to reduce the psycho-visual redundancy, larger and smoother quantization coefficients in middle-high frequencies are used in JPEG quantization matrices for chrominance, compared with that for luminance. As a result, the decoded color components are smoother because more similar local chrominance is obtained.

When a photograph is tampered, the manipulation such as blurring modifies the values of hue and introduces distortion of color coherence[11].

III. Feature Extraction

In order to make our discussion clearly, we consider the following scenario: the forger first pastes a photograph with an object that is cut from another image and resized to proper resolution, then blurs the whole object to remove the trace of tampering, and finally obtain a sophisticated forgery called a copy-paste-blur one. Without restricting generality, we choose HSI as the color space in this paper. In order to localize the tampered region, all of the features described below are extracted from sub-images, which are generated by dividing the test image into several blocks.

1. Cardinality features of the Hue

For a photographic image I with $M \times N$ pixels, the color coherence can be indicated by the same hue values in a local region. When the copy-paste-blur tampering occurs, the manipulations introduce distortion of the coherence, which makes the hue value $h_{i,j}$ at the pixel location (i, j) possibly different from its neighbors. In our test, we straightforward use the ratio of cardinality of the hue set to the total number of pixels:

$$f_1 = |H_I|/MN \tag{4}$$

where H_I indicates the set of hues and $|\cdot|$ means calculating the cardinality of a set. The numerical precision of the hue values used here and following is automatically defined by the implementation software, Matlab 7.0.

To capture an insensitive feature to different cameras and contents, we employ a predictor to estimate the increment of the cardinality of the hue set for the photographic image. The predictor aims to simulate the processing of blurring, which introduces distortion of the color coherence. In our work, a Gaussian filter which is empirically set to size of 5×5 with a standard deviation $\sigma = 0.5$ is applied to the image to produce a predicted one $F(I)$. The consideration of using Gaussian filter as predictor of blurring is based on the observation that most blurring process could be modeled as a low-pass Gaussian filter[12]. The ratios of cardinality of hue set to image size for I and $F(I)$ are then calculated separately. We take the difference between the two ratios as the predictive feature:

$$f_2 = |H_{F(I)}| - |H_I|/MN \tag{5}$$

where $H_{F(I)}$ indicates the set of hues in the filtered photograph.

2. Statistical features of the AHR

We characterize color coherence in local region through Abnormal hue ratio (AHR). For the photographic image I, we first divide it into L blocks with $K \times K$ pixels, and then the AHR of all blocks are computed separately. The AHR is defined as the ratio of the number of abnormal hues to the block size. Abnormal hue (AH) means that the value of the hue appears individually in the block. We take the ratio of the variance to the mean as the third statistical feature:

$$f_3 = \frac{1}{L}\sum_{i=1}^{L}\left(AHR_i - \frac{1}{L}\sum_{i=1}^{L}AHR_i\right)^2 \Bigg/ \frac{1}{L}\sum_{i=1}^{L}AHR_i \tag{6}$$

where AHR_i indicates the AHR of ith block. This feature indicates the distortion of the coherence in local region while tampering.

To suppress the effect of the noisy and overexposed pixels, we take the mean and variance of the 5% blocks associate with largest AHR, as the last two features:

$$f_4 = \frac{1}{\lfloor 0.05L \rfloor}\sum_{i=1}^{\lfloor 0.05L \rfloor} AHR_i^{\max} \tag{7}$$

$$f_5 = \frac{1}{\lfloor 0.05L \rfloor}\sum_{i=1}^{\lfloor 0.05L \rfloor} (AHR_i^{\max} - f_4)^2 \tag{8}$$

where $AHR_i^{\max}$ indicates the ith maximum AHR in all L blocks. Finally, we obtain a vector consist of 5 features.

IV. Experiments

1. Experimental parameters

In our experiments, the samples for training in the classifier are chosen randomly from 13 different digital camera models, and the testing samples are obtained from another 20 digital cameras[13], which are assumed inaccessible to the analyst. Table 1 shows all of the digital camera models.

To localize the tampered region, all of the photographs are divided into several sub-images. The sub-image cannot be too small to avoid the lack of statistically significant data, and also not be too large because then the accuracy of tampered region localization is less likely to be held. For typical photograph no less than 1 million pixels, we recommend the sub-image with 128 × 128 pixels and the blocks are specified as 8 × 8 pixels.

LIBSVM[14] is taken as the classifier. We use C-Support vector classification (C-SVC) with non-linear RBF kernel, which is defined as $K(x_i, x_j) = \exp(-\gamma||x_i - x_j||^2)$, where x_i and x_j denote corresponding features of the ith and jth samples respectively. The parameter (C, γ) can be determined by a grid search using cross validation[15].

Table 1. Digital cameras used in experiments

ID	Camera	ID	Camera
1	Canon EOS 400D	18	Casio EX-Z750
2	Casio EX-Z1000	19	Fuji Finepix S3 Pro
3	Fuji FinePix F300	20	Kodak DX7590
4	Fuji FinePix S1 Pro	21	Kodak EasyShare P880
5	Fuji FinePix S6500	22	Kodak P850
6	Nikon E8800	23	Nikon D80
7	Nikon D200	24	Olympus SP500UZ
8	Olympus E-300	25	Olympus SP-310
9	Panasonic DMC-FZ50	26	Olympus SP-550UZ
10	Pentax K100D	27	Panasonic DMC-L1
11	Pentax Optio 750Z	28	Panasonic LX2
12	Sony DSC-H5	29	Samsung NV7 OPS
13	Sony DSLR-A100	30	Kodak DC290
14	Canon EOS 5D	31	Nikon E5700
15	Canon Powershot A640	32	Canon Pro1
16	Canon Powershot SD800	33	Sony DFS-828
17	Casio EX-P700		

To create a forgery, we copy the tampered object, and paste another photograph with it in Adobe Photoshop, edition of 8.0.1. After that, we use the blurring tools on the object to eliminate the discontinuity of the splicing. The master diameter in our experiments is set from 30 to 100 according to the size of copy-paste object, and the hardness and strength are set to the default values. Several samples are illustrated in middle column in Fig.3.

2. Experimental results

We choose 12 photographs stochastically from each of the cameras (ID 1-13). The 156 photographs are then divided into 30715 sub-images. The features of each sub-image and its blurred counterparts are fed to the SVM. There are 864 authentic photographs and 779 copy-paste-blur forgeries from another 20 cameras (ID 14-33) used for test.

The True positive rate (TPR) and True negative rate (TNR) are used as measures to quantify the performance of the classification system. In our work, the TPR represents the ratio of authentic pixels which are actually classified as authentication, and TNR indicates the ratio of forgery pixels which are correctly classified as forgeries. Table 2 tabulates the TPR and TNR performance of classification, and intuitionistic results are illustrated in Fig.3.

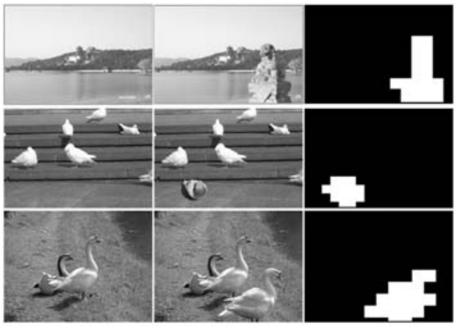


Fig. 3. Shown in rows are authentic photographs (the left), the forgeries (the middle), and the detection results (the right)

Table 2. Accuracy of the proposed scheme

Overall classification accuracy	TPR	97.1%
	TNR	96.4%

Finally, we list the detection rates achieved by applying the different features alone in Table 3 to evaluate the efficiency of the 5 features separately. After that, the Sequential forward feature selection (SFFS) algorithm[16] is employed to examine how efficient the different combination of the features is. Fig.4 shows that the best accuracy of 96.8% is achieved by all of the 5 features, though an acceptable detection rate of 90.4% is obtained for the combination of 3 features.

Table 3. Detection rates for the individual features

Feature	f_1	f_2	f_3	f_4	f_5
TPR	77.5%	82.1%	66.6%	88.3%	72.3%
TNR	61.8%	92.2%	76.2%	84.2%	83.5%
Accuracy	69.7%	87.2%	71.4%	86.3%	77.9%

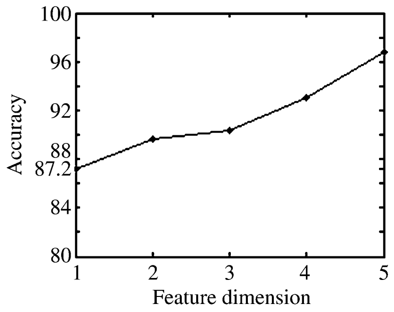


Fig. 4. Detection rate for the combination of different features

V. Conclusions

In this paper, we propose a novel approach for copy-paste-blur detection, based on extracting statistical features of color coherence. We first discuss the color coherence introduced by CFA interpolation and JPEG compression. A vector of 5 features is proposed as the input of the SVM classifier. By dividing photograph into several sub-images, we build a forensic detector that can localize the tampered region in high accuracy.

In our future work, we will investigate some other manipulations used for forgery making, such as sharpening, contrast stretching and so on. We are also looking forward to extending this approach for re-sampling detection.

References

[1] A. Swanminathan, M. Wu, K.J.R. Liu, "Component forensics of digital cameras: a non-intrusive approach", *Proc. of IEEE Conference on Information Science and System*, Princeton, New Jersey, USA, pp.1194–1199, 2006.

[2] A.C. Popescu, H. Farid, "Exposing digital forgeries by detecting duplicated image regions", *Technical Report*, Dartmouth College, Computer Science, 2004.

[3] J. Fridrich, D. Soukal, J. Lukáš, "Detection of copy-move forgery in digital images", *Proc. of Digital Forensics Research Workshop*, Cleveland, USA, 2003.

[4] T.T. Ng, S.F. Chang, "A model for image splicing", *Proc. of IEEE ICIP*, Singapore, pp.1169–1172, 2004.

[5] T.T. Ng, S.F. Chang, Q. Sun, "Blind detection of photomontage using higher order statistics", *Proc. of IEEE International Symposium on Circuits and Systems*, Vancouver, Canada, pp.688–691, 2004.

[6] H. Farid, "Detecting digital forgeries using bispectral analysis", *Technical Report*, Cambridge, MIT AI Memo, 1996.

[7] J. Lukáš, J. Fridrich, M. Goljan, "Digital "bullet scratches" for images", *Proc. of IEEE ICIP*, Genova, Italy, pp.2637–2640, Sept. 2005.

[8] J. Lukáš, J. Fridrich, M. Goljan, "Detecting digital image forgeries using sensor pattern noise", *Proc. of Security, Steganography, and Watermarking of Multimedia Contents VIII, SPIE Electronic Imaging.* San Jose, California, USA, pp.362–372, 2006.

[9] J. Adams, K. Parulski, K. Spaulding, "Color processing in digital cameras", *IEEE Micro*, Vol.18, No.6, pp.20–30, 1998.

[10] J. Lukas, J. Fridrich, M. Goljan, "Determining digital image origin using sensor imperfections", *Proc. of Conference on Image and Video Communications and Processing*, San Jose, California, USA, pp.249–260, 2005.

[11] A. Popescu, H. Farid, "Exposing digital forgeries in color filter array interpolated images", *IEEE Transactions on Signal Processing*, Vol.53, No.10, pp.3948–3959, 2005.

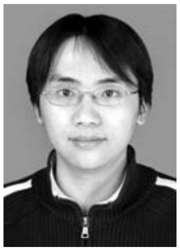
[12] S. Bayram, I. Avcibas, B. Sankur, "Image manipulation detection", *Journal of Electronic Imaging*, Vol.15, No.4, pp.1–17, 2006.

[13] Digital Photography Review, http://www.dpreview.com/.

[14] C.C. Chang, C.J. Lin, "LIBSVM: A library for support vector machines", http://www.csie.ntu.edu.tw/∼cjlin/libsvm, 2008-10-13.

[15] C.W. Hsu, C.C. Chang, C.J. Lin, "A practical guide to support vector classification", http://www.csie.ntu.edu.tw/∼cjlin/papers/guide/guide.pdf, 2008-05-21.

[16] P. Pudil, F.J. Ferri, J. Novovicova, J. Kittler, "Floating search methods for feature selection with nonmonotonic criterion functions", *Proc. of 12th IEEE Int. Conf. on Pattern Recognition*, Jerusalem, Israel, pp.279–283, 1994.



WANG Bo received the B.S. degree in electrical engineering from Dalian University of Technology, Dalian, China, in 2003, and is currently pursing the Ph.D. degree in signal and information processing at the Department of Electronic and Information Engineering, Dalian University of Technology. His research interests include information security and multimedia forensics. (Email: dlut.wangbo@gmail.com)

KONG Xiangwei is a professor of Department of Electronic and Information Engineering, and vice-director of Information Security Research Center of Dalian University of Technology, Dalian, China. She is also the vice-director of the multimedia security session of Chinese Institute of Electronics. Her research interests include information security and forensics, multimedia signal processing and multi-information fusion. (Email: kongxw@dlut.edu.cn)

Elisa Bertino is a professor of the Department of Computer Sciences, Purdue University, America, and Research Director of CERIAS. Her main research interests cover the fields of information security and database systems. She is co-editor in chief of VLDB Journal and is currently a member of the editorial board of several international journals, including ACM Transaction on Information and System Security, IEEE Internet Computing, IEEE Security and Privacy *etc.* (Email: bertino@cerias.purdue.edu)

FU Haiyan received the B.S. degree in electrical engineering from Qufu Normal University, Shandong, China, in 2003, and the M.S. degree from Dalian University of Technology, Dalian, China, in 2006. She is currently pursing the Ph.D. degree in signal and information processing at the Department of Electronic and Information Engineering, Dalian University of Technology, where she works as an assistant since 2006. Her current research focuses on the multimedia signal processing and image retrieval in e-business. (Email: fuhy@dlut.edu.cn)