휴대폰의 CFA 패턴특성을 이용한 사진 위변조 탐지

심재연, 김성환
서울시립대학교 컴퓨터과학부
e-mail : simpo@uos.ac.kr, swkim7@uos.ac.kr

Automatic Detection of Forgery in Cell phone Images using Analysis of CFA Pattern Characteristics in Imaging Sensor

Jae-Youen Shim and Seong-Whan Kim
Dept. of Computer Science, University of Seoul

Abstract

With the advent of cell phone digital cameras, and sophisticated photo editing software, digital images can be easily manipulated and altered. Although good forgeries may leave no visual clues of having been tampered with, they may, nevertheless, alter the underlying statistics of an image. Most digital camera equipped in cell phones employ a single image sensor in conjunction with a color filter array (CFA), and then interpolates the missing color samples to obtain a three channel color image. This interpolation introduces specific correlations which are likely to be destroyed when tampering with an image. We quantify the specific correlations introduced by CFA interpolation, and describe how these correlations, or lack thereof, can be automatically detected in any portion of an image. We show the efficacy of this approach in revealing traces of digital tampering in lossless and lossy compressed color images interpolated with several different CFA algorithms in test cell phones.

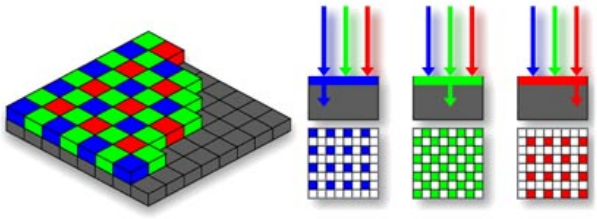
1. Introduction

With the advent of cell phone digital cameras and sophisticated editing software, digital images can be easily manipulated and altered. Digital forgeries, often leaving no visual clues of having been tampered with, can be indistinguishable from authentic photographs. As a result, photographs no longer hold the unique stature as a definitive recording of events. Of particular concern is how the judicial system and news-media will contend with this issue. How many of the images that we see every day have been digitally doctored.

We describe a technique for detecting traces of digital tampering in the complete absence of any form of digital watermark or signature. This approach works on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may, nevertheless, alter the underlying statistics of an image. For example, consider the creation of a digital forgery that shows a pair of famous movie stars, rumored to have a romantic relationship, walking hand-in-hand. Such a photograph could be created by splicing together individual images of each movie star and overlaying the digitally created composite onto a sunset beach. In order to create a convincing match, it is often necessary to resize, rotate, or stretch portions of the images. This process requires re-sampling the original image onto a new sampling lattice. Although this re-sampling is often imperceptible, it introduces specific correlations into the image, which when detected can be used as evidence of digital tampering. We describe the form of these correlations, and how they can be automatically detected in any portion of an image. We show the general effectiveness of this technique and analyze its sensitivity and robustness to counter-attacks.

2. Related Work

CFA based CCD (Charge-coupled Devices) and CMOS (Complementary Metal-Oxide Semiconductor) are usually used digital camera image sensors. CFA is a mosaic of tiny color filters placed over the pixel sensors of an image sensor to capture color information. Most CFA are arranged with Bayer filter style. Bayer filter mosaic is arranging RGB color filters on a square grid of photo sensors. The filter pattern is Green 50%, Red 25%, Blue 25%, GRGB or RGGB style. Each sensor gets color information with interpolation of neighbor color information [1].



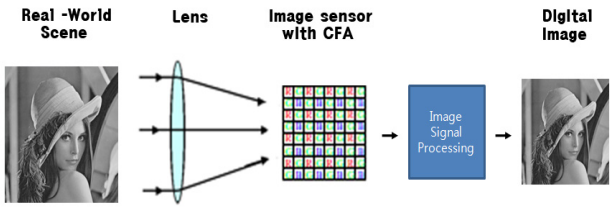
(Figure 1) The basic idea of CFA

The information saves with RGB color data. General interpolation methods have two base-type. One is Bilinear based method another is Gradient based method. Bilinear based method use neighborhood data information with

special filters, and Gradient based method use neighbor-hood data information with vertical and horizontal directions values.

CCDs are usually used memory storage or shift register because it can move to low electric potential of semiconductor surface with electric charge. Photo-detector is called potential well because photo-detector stores light. Those stored volts are emitted with timing signal. Stored lights are changed to electrons and those electrons are changed to voltages. Photo-detectors on CCD image sensor are saved just light size like contrast. It shows gray color image. So we need another changing method for color image, and we get information of color image using CFA. CMOS image sensors are implemented using PMOS and NMOS transistors. It uses low electrical energy. CMOS transistors are integrated each photo-detector and change light that are saved by photo-detector to electric charge. CCD amplify sequential signal through the photo diode and CFA but each CMOS pixel has signal amplification device. So CCD has small chip size and low signal loss and high electricity consumption but CMOS has high speed process and low electricity consumption and normally high signal loss. CMOS has more noise than CCD but most cell phone camera image sensors use CMOS type because CMOS has small chip size and low price.

When a real-world scene is captured using a digital cell phone camera, the information about the scene passes through the various cell phone camera components before the final digital image is produced. The light from the scene pass through the lens and the optical filters and is finally recorded by the color sensors. The CFA consists of an array of color sensors, each of which captures the corresponding color of the real-world scene at an appropriate pixel location. Since only a single color sample is recorded at each pixel location, the other two color samples must be estimated from the neighboring samples in order to obtain a three-channel color image. Each of these cell phone camera components, such as color filter array and color interpolation employ a particular set of algorithms with an appropriate set of parameters to modify the input scene. Each of these cell phone camera components, such as color filter array and color interpolation employ a particular set of algorithms with an appropriate set of parameters to modify the input scene.



(Figure 2) Digital camera image processing

Recently, several different methods for detecting digital forgeries were proposed. Ng and Chang proposed a method for detection of photomontages [2]. Popescu et al. developed several methods for identifying digital forgeries by tracing artifacts introduced by re-sampling [3] and Color Filter Array (CFA) interpolation [4]. Recently, Johnson et al. proposed another method based on inspecting inconsistencies in lighting conditions [5]. Fridrich et al. established a method for detecting copy-move forgeries [6]. A.N. Myna et al. proposed using wavelets for detecting digital forgeries [7]. Lukáš et al. proposed method based Sensor Pattern Noise [8]. For each of these methods, there are circumstances when they will fail to detect a forgery. Method [2], for instance, has very restricting assumptions that are usually not fulfilled and even when they are satisfied its misclassification rate is almost 28%. The copy-move detection method [6] is limited to one particular case of forgeries, when a certain part of the image was copied and pasted somewhere else in the same image. Methods based on detecting traces of re-sampling may produce less reliable results for processed images stored in the JPEG format. The method based on detection of inconsistencies in lighting assumes nearly Lambertian surface for both the forged and original areas and might not work when the object does not have a compatible surface, when pictures of both the original and forged objects were taken under approximately similar lighting conditions, or during a cloudy day when no directional light source was present.

3. Design of Forgery Detection Scheme

In this paper, we present a scheme for detecting forgeries using cell phone camera image forgeries based on the unique characteristics of cell phone camera image sensor. Our scheme consist of three stages: (1) we detect specific characteristics in image, (2) we use EM algorithm for estimates map to image modeling and we found specific peaks the magnitude of the Fourier transform of estimates map, and (3) we detect image forgeries location.

3.1. Detection of specific characteristics in cell phone camera image

Most cell phone camera image sensor use CMOS. Characteristics of CMOS are high signal loss and a lot of noise. We try to find those CMOS Characteristics and detect sensor pattern noise and estimate CFA interpolation method for cell phone camera image forgeries detecting. First we use de-noise filter to cell phone camera image for image sensor pattern noise detecting. We applied Independent Component Analysis (ICA) based Gaussian noise filtering (de-noising) instead of Wiener filter. From the Bayesian viewpoint Wiener filter is an inference method which computes Maximum Likely (ML) estimates of image signal given the noise variance. Wiener filter assumes Gaussian distribution for both original image and noise. But real image statistics are much different from Gaussian distribution and are better modeled by the ICA model. If the ICA model provides better approximation of real image signals, then it can dramatically enhance noise filtering and detection. ICA is an unsupervised learning method which has found wide range of applications in image processing [9].

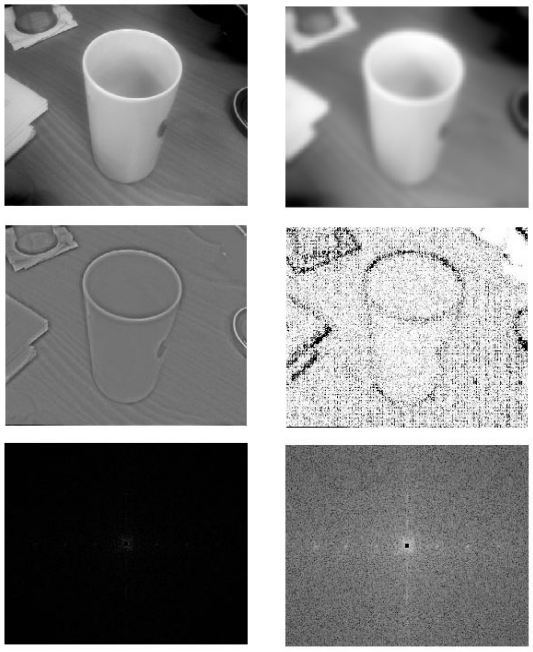
Image $f(x, y)$ has original signals $s(x, y)$ and noises $n(x, y)$. This process can be sped up by suppressing the scene content from the image, which can be achieved using a de-noising filtered image $s`(x, y)$ and the noise residuals $n`(x, y)$.

$$f(x, y) = s(x, y) + n(x, y)$$
$$s`(x, y) = g(x, y) * [\, s(x, y) + n(x, y) \,]$$
$$n`(x ,y) = f(x, y) - s`(x, y)$$

We use this n`(x, y) for estimates map, that included nosic and edge. We can estimates using that to image sensor pattern nosic.

3.2. EM Algorithm for Unique Pattern Trace

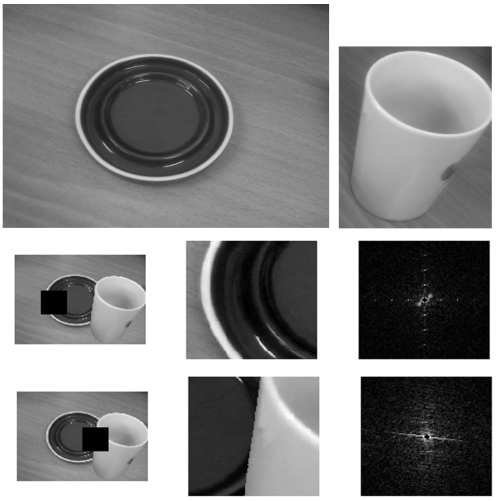
We employ the expectation/maximization algorithm (EM) [10] to simultaneously estimate a set of periodic samples that are correlated to their neighbors, and the specific form of these correlations. We can make estimates map CFA pattern specific characteristics and color interpolation with EM algorithm. And using this estimates map we can detect image forgeries and demonstrate image forgeries. The EM algorithm is a two-step iterative algorithm, E-step, the probability that each sample belongs to each model is estimated and M-step, the specific form of the correlations between samples is estimated. M- step estimate maximum likelihood of data using E-step data. In this paper, E-step estimate the probability of each sample, obtained using Bayes' rule. Because most CFA of mobile phome image sensor use Bayer Filter. Using EM algorithm we make estimates map from estimated image maximum likelihood. And 2D-Fourier transform is applied estimates map to find pattern peak of image. We use that for detecting image forgeries.



(Figure 3) Top are original and de-noising image, middle are image noise and estimates map, bottom are two type of Fourier transform of estimates map

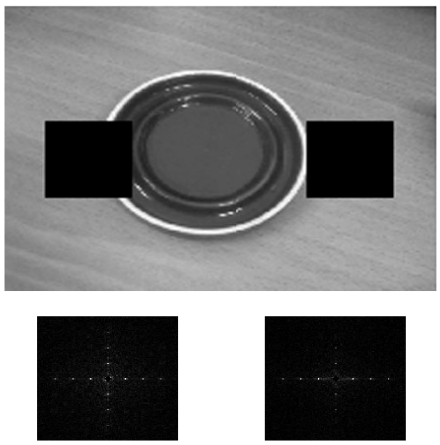
3.3. Detection of Image Forgeries

For image forgeries ROI, we divide the image in blocks and detect image peak pattern using Fourier transform of estimates map of each block. In this paper, we proposed block cross section for image forgeries to detecting variety forgeries size and image size. We process this action that makes more reliability and accuracy detecting forgeries in image.



(Figure 4) Top are original and synthesis source image, middle are non- forgeries image estimates location bottom are forgeries image estimates location

Also we confirm the each non- forgeries image blocks shows similar peak pattern



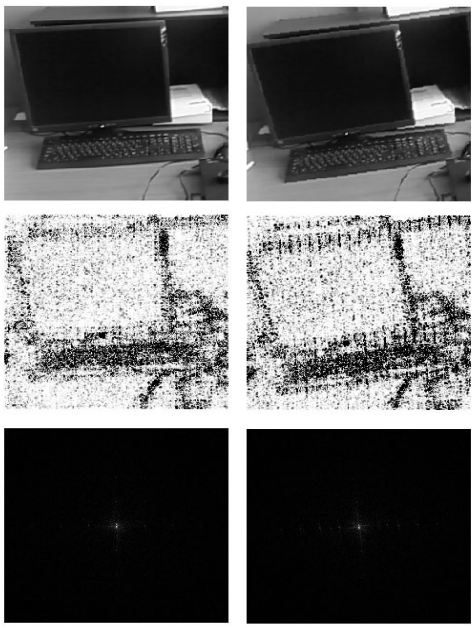
(Figure 5) The peaks in the Fourier transform correspond to the presence of CFA interpolation in the image. These patterns are present in all regions of the image

4. Experimental Results

In this paper, we collected one hundred images with Green color channel and set to store the images in uncompressed TIFF format. Image sizes are using normal cell phone camera used size we use ten kind of mobile camera device. Normally mobile camera image file format is JPEG but we use TIFF format after forgeries. We proposed 3x3 size coefficients filter for estimates map. We detect image forgeries. We use Green color channel of images for image modeling and MATLAB 7.9.0 for system processing.

4.1. Detection of Rotation

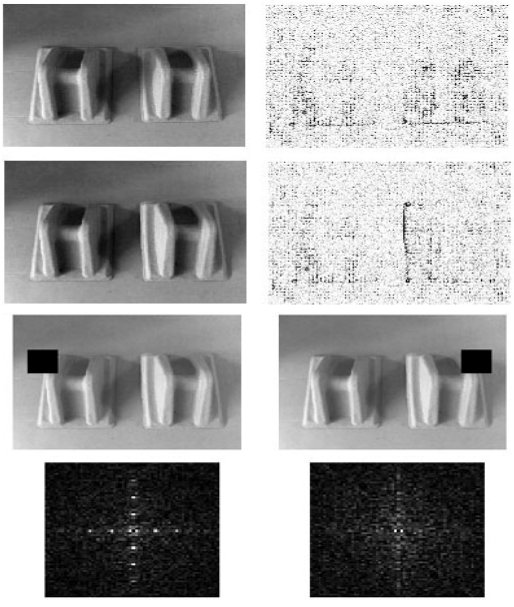
For cell phone camera image forgeries usually do re-sampling for changing image size or rotating for changing image objects location, also delete or erase image objects. Most image forgeries affairs, images join other images after that. We detect specific characteristics of rotated image and find turn of peak pattern.



(Figure 6) Top are original image, and the same image rotated by 5. Middles are estimates maps and bottoms are Fourier transform of each estimates map

4.2. Detection of Forgeries using Same Camera Images

In forgeries synthetic image from the same camera case we can estimate pattern slip for image forgeries using our proposed system. In this case, most forgeries image has cut performance with slip image pattern. In this location we can see changing pattern peak with 2-D Fourier transform.



(Figure 7) Original image and a forgery

5. Conclusion

Most cell phone cameras employ a single sensor in conjunction with a color filter array (CFA), where the missing color samples are then interpolated from these recorded samples to obtain a three channel color image. This interpolation introduces specific correlations which are likely to be destroyed when tampering with an image. As such, the presence or lack of correlations produced by CFA interpolation can be used to authenticate an image, or expose it as a forgery. We have shown, for eight different CFA interpolation algorithms, that a simple linear model captures these correlations. We have also shown the efficacy of this approach to detecting traces of digital tampering in lossless and lossy compressed images.

As with any authentication scheme, our approach is vulnerable to counter-attack. A tampered image could, for example, be re-sampled onto a CFA, and then re-interpolated. This attack, however, requires knowledge of the camera's CFA pattern and interpolation algorithm, and may be beyond the reaches of a novice forger.

We are currently exploring several other techniques for detecting other forms of digital tampering. We believe that many complementary techniques such as that will be needed to reliably expose digital forgeries. There is little doubt that even with the development of a suite of detection techniques, more sophisticated tampering techniques will emerge, which in turn will lead to the development of more detection tools, and so on, thus making the creation of forgeries increasingly more difficult.

Acknowledgement

본 연구는 문화체육관광부 및 한국문화콘텐츠진흥원의 2009 년도 문화콘텐츠산업기술지원사업의 연구결과로 수행되었음

REFERENCES

[1] http://www.wikipedia.org
[2] Ng T.-T. and Chang S.-H. “Blind Detection of Digital Photomontages using Higher Order Statistics”, ADVENT Technical Report #201-2004-1, Columbia University, June 2004.
[3] Popescu A.C. and Farid H. “Exposing Digital Forgeries by Detecting Traces of Resampling”, IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.
[4] Popescu A.C. and Farid H. “Exposing Digital Forgeries in Color Filter Array Interpolated Images”, IEEE Transactions on Signal Processing, vol. 53(10), pp. 3948–3959, 2005.
[5] Johnson M.K. and Farid H. “Exposing Digital Forgeries by Detecting Inconsistencies in Lighting”, Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.
[6] Fridrich J., Soukal D., and Lukáš J. “Detection of Copy-Move Forgery in Digital Images”, Proc. Digital Forensic Research Workshop, Cleveland, OH, August 2003.
[7] A.N. Myna, M.G. Venkateshmurthy, C.G Patil, "Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping", International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), vol. 3, pp.371-377, 2007.
[8] Jan Lukáš, Jessica Fridrich, and Miroslav Goljan, “Detecting digital image forgeries using sensor pattern noise Proceedings of SPIE. Vol. SPIE-6072, pp. 362-372. 2006.
[9] Seong-Whan Kim and Hyun-Sung Sung "Perceptually Tuned Auto-correlation Based Video Watermarking Using Independent Component Analysis", PCM 2005, Part II, LNCS 3768, pp. 360 – 370, 2005.
[10] A. Dempster, N. Laird, and D. Rubin, "Maximum lilelihood from incomplete data via the EM algorithm", J. Roy. Statist. Soc., vol. 99, no. 1, pp. 1–38, 1977.
[11] H. Farid and S. Lyu, "Higher-order wavelet statistics and their application to digital forensics," in IEEE Workshop on Statistical Analysis in Computer Vision, Madison, Wisconsin, 2003.