HUE MODIFICATION ESTIMATION USING SENSOR PATTERN NOISE

Jong-Uk Hou *Han-Ul Jang* *Heung-Kyu Lee*†

Korea Advanced Institute of Science and Technology, Republic of Korea

ABSTRACT

In digital image forensics, previous methods for hue forgery detection cannot be used after common image processing such as resizing and JPEG compression. In this paper, we suggest a robust forensics scheme for estimating hue modification of images. To achieve this goal, we use sensor pattern noise from each color channel of untampered images as the ground truth. Since we know the unique characteristics of each color channel, we can estimate a hue modification by testing suspicious images for all hue changes. The results confirms that the proposed method distinguishes hue modification and estimates the changed degree; moreover, it provides robustness against resizing and JPEG compression.

Index Terms— Digital image forensics, Hue, Hue modification, Sensor pattern noise, Color Filter Array

1. INTRODUCTION

In the age of high performance digital cameras and the Internet, digital images have become one of the most widely used information sources. Unlike text, an image is an effective and vivid communication medium for people to understand content easily by stimulating their visual system. However, digital images can be easily falsified by non-professional users, especially since the advent of high-quality image editing tools such as Adobe Photoshop, Paintshop Pro, etc. Therefore, the demand for digital image forensics that identifies forgeries in digital images has significantly increased.

One of the common forgeries in digital images is hue modification. Hue is a main property of a color, therefore, the counterfeiters who attempt to tamper with the color attribute usually change the hue. With an image editing tool, someone can severely distort the actual meanings of images by modifying the hue of the images. Using social network services such as Flickr, Instagram, and Pinterest, it is simple to distribute the distorted ideas and information with digital images. In second-hand markets such as auction, the hue modification can easily occur. For instance, someone who wants to sell his/her mobile or car modifies the color of the item to better attract the customer (See Fig.1).

†: Corresponding Author: hklee@mmc.kaist.ac.kr

(a) Original image (b) Forged image

Fig. 1. Image of iPhone-5c was tampered with hue modification. Color of iPhone is changed to pink.

For example, with severe hue modification, media may broadcast the perverted truth of a particular accident by changing the hue of the images that were are shot at the accident site. For example, the German-language daily tabloid Blick forged an image by changing the color of the flooding water to blood-red so that it appeared to be blood and distributed the falsified image to news channels [1].

To cope with this kind of forgery, Choi et al. [2] proposed a color modification estimation algorithm using a neighboring correlation by a color filter array (CFA) in a digital camera. However, Choi's algorithm cannot be used after common image processing, such as resizing and JPEG compression in which the neighboring correlation of an original image is completely broken.

In this paper, we suggest a robust forensics scheme for estimating a hue modification. The scheme distinguishes a hue modification by using sensor pattern noise and estimates the changed degree; moreover, it provides robustness against resizing and JPEG compression.

The rest of this paper is organized as follows. Section 2 briefly introduces the background knowledge, and Section 3 explains the details of the proposed method. To demonstrate the performance of the proposed scheme, we tested our method with various image data sets in Section 4, and Section 5 presents the conclusion.

2. BACKGROUNDS

2.1. Image capturing process

Fig. 2 demonstrates the process of capturing images using a digital camera. Light is represented by three color components: R,G, and B. Light from the scene passes through

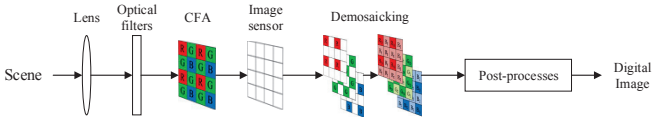


Fig. 2. Image capturing process of a digital camera.

the lens which transmits the light by converging it. For every pixel light, one color component of three color components passes through a color filter array (CFA) and is subsequently converted to electronic signals by an image sensor. After image sensing, the two components that were not sensed are created by demosaicing using signals of neighboring pixels. Then, signals of every pixel undergo post-processing such as white balance, gamma correction, and image enhancement. Finally, the signals are stored in the memory of a camera in a customized format.

While an image is being processed, the signal is inevitably distorted as it passes through each process. Due to these distortions, slight differences between the real scene and the captured image occur [3].

2.2. Sensor pattern noise (SPN)

Sensor pattern noise (SPN) has received attention for digital camera identification because it distinguishes device models as well as individual devices of the same model. SPN consists of fixed pattern noise (FPN) and photo response non-uniformity (PRNU). The FPN is caused by dark currents and is suppressed by subtracting the dark frame.

The dominant component of SPN is PRNU [3]. PRNU is mainly caused by the inhomogeneity of silicon wafers and light variations in which individual sensor pixels convert light to electrical signals [4]. Every sensor, thus, generates a unique SPN whenever an image or a video is shot. Therefore, SPN performs as a sensor fingerprint that verifies images in the field of digital image forensics [5–8].

2.3. Hue modification

In the polar coordinate representations of the RGB color space, hue is the degree to which a stimulus can be described as similar to or different from stimuli that are described as red, green, blue, and yellow [9]. Preucil describes a color hexagon [10] that can be used for computing the hue of images in the RGB channel, as shown in Eq. 1.

$$\tan(hue) = \frac{\sqrt{3} \cdot (G - B)}{2 \cdot R - G - B}. \quad (1)$$

In the hexagon, red is placed at 0°, green at 120°, and blue at 240°. Hue is a main property of a color, the counterfeiters who attempt to tamper with a color attribute usually change the hue. Hue modification is described as exchanging intensities between all the color channels. As shown in Fig 3, the intensity of each color channel may be exchanged directly or recombined depending on the degree of modification. In addition, a pixel generally preserves its luminance while modifying the hue attribute.

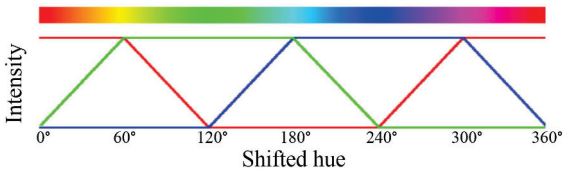


Fig. 3. Relationship between hue of colors and their corresponding RGB intensity.

3. PROPOSED METHOD

3.1. Reference patterns for each color channel

As explained in Section. 2.1, the raw output of the image sensor was separated into three color components by a color filter array. The SPN, the unique fingerprint of a digital camera, was also separated through this process. Fig. 4 shows an example of the SPN separation by the Bayer pattern [11], the most widely used pattern in a digital camera. Each separated SPN forms a pattern independent of the others, since the positions of each SPN were not overlapped. For example, as shown in Fig. 4, noise residual N00 is included in red channel, but not in blue and green channel. Therefore, the SPN of each color channel represents a unique characteristic of each untampered color channels.

In order to extract the SPN, Lukas et al. [3] proposed a scheme to obtain an approximation of the SPN. Using this method, we can obtain the SPN of each color channel P_c by averaging multiple untampered images $I_c^{(k)}$ where $k = 1, ..., N_p$ and $c \in \{R, G, B\}$. R, G and B denote the red, green, and blue color channels, respectively. The obtained SPN P_c for each color channel c is used as a color reference pattern, which represents a unique characteristic of each untampered color channel.

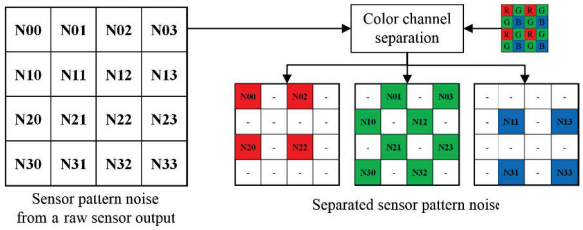


Fig. 4. Sensor pattern noise separation by CFA Bayer pattern.

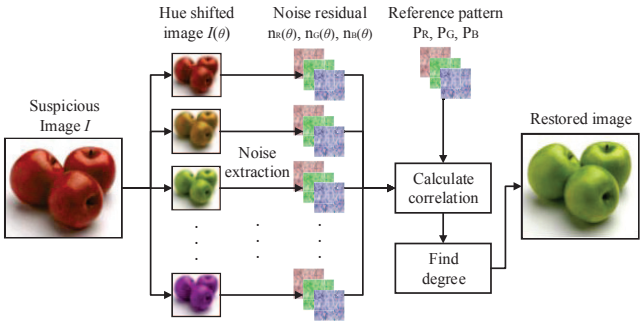


Fig. 5. Overall process of the proposed method.

3.2. Color modification estimation process

The overall procedure of the proposed method is described in Fig. 5. First, the hue value of the suspicious image I was shifted from $0°$ to $359°$, and we obtained hue shifted suspicious image $I(\theta)$. We then extract a color noise residual $n_c(\theta)$ from each color channel c of $I(\theta)$ using a wavelet-based denoising filter [3].

Because of the noise-like character of the SPN, detecting its presence in each color channel is possible using correlation [3]. Therefore, in order to detect the presence of reference pattern P_c in a suspicious image, we calculated the correlation $\rho_c(\theta)$ between the color noise residual $n_c(\theta)$ and the color reference pattern P_c as follows:

$$\rho_c(\theta) = corr(n_c(\theta), P_c) = \frac{(n_c(\theta)-\overline{n_c(\theta)})\cdot(P_c-\overline{P_c})}{\|n_c(\theta)-\overline{n_c(\theta)}\|\cdot\|P_c-\overline{P_c}\|}, \quad (2)$$

where the bar above a symbol denotes the mean value.

If the hue shift in the suspicious image I was reversed by the same amount of tampering, each color noise residual $n_c(\theta)$ has the maximum correlation with P_c. For example, when the hue of the original image was changed by $120°$, the intensities in the red and blue channels were swapped (see Section 2.3). In this case, the noise residual from the blue channel n_B had the maximum correlation with P_R, but not with P_B. Only after we shifted the hue of the suspicious image I to be reversed by $-120°$, did the n_B have the maximum correlation with P_B.

Therefore, using the $\rho_c(\theta)$ values calculated above, the degree of the hue shift $\hat{\theta}$ was estimated as the following equation:

$$\hat{\theta} = \underset{\theta}{\operatorname{argmax}}[\sum_c(\rho_c(\theta))]. \quad (3)$$

If the estimated degree $\hat{\theta}$ was zero, the suspicious image did not undergo any hue modification. In contrast, if the $\hat{\theta}$ was non-zero, the hue of the suspicious image was modified. In this case, we could restore the hue tampered image using $-\hat{\theta}$ hue shifting.

4. EXPERIMENTAL RESULTS

4.1. Experimental setup

For our experiment, we used sample raw images collected from the *Dresden Image Database* [12] for digital image forensics. The rest of the raw images were taken directly using the camera models. Table 1 depicts the details of the image database. All raw images were interpolated by *dcraw*, the most widely used raw image decoder, using adaptive homogeneity-directed (AHD) interpolation algorithms [13]. The hue of the sample images was shifted from $0°$ to $359°$ in steps of $57°$ to generate test images.

For evaluating accuracy, the root mean square error (RMSE) was adopted.

$$RMSE = \sqrt{E((\hat{\theta}-\theta)^2)} \quad (4)$$

θ and $\hat{\theta}$ represent the actual degree of hue modification and the estimated degree, respectively. RMSE serves to aggregate the magnitudes of the errors in estimations for various experiments.

Model	# images	Resolution	CFA pattern
Nikon D200	200	3904×2616	RGGB
Nikon D70	200	3040×2014	BGGR
Nikon D70s	200	3040×2014	BGGR
Nikon D90	100	4352×2868	GBRG
Canon EOS 7D	100	5202×3465	RGGB
Canon EOS 400D	100	3906×2602	RGGB
Olympus E420	100	3720×2800	RGGB

Table 1. Digital camera models in our experiments

4.2. Hue modification estimation result

Fig. 6 depicts the plot of the RMSE values versus the different number of the images N_p for the reference pattern. The results of the proposed method are acceptable even though $N_p < 5$. These are notable results compared to other methods [3,5] using SPN recommended $N_p > 50$ for the reasonable results. In our method, unlike the other techniques, SPN is only used for comparison between correlations for each color channel. Therefore, a relatively small amount of SPN information is required for detecting hue modification.

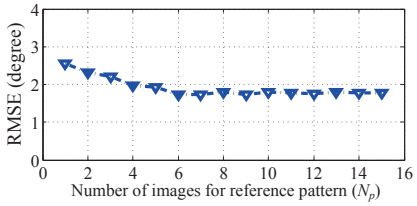
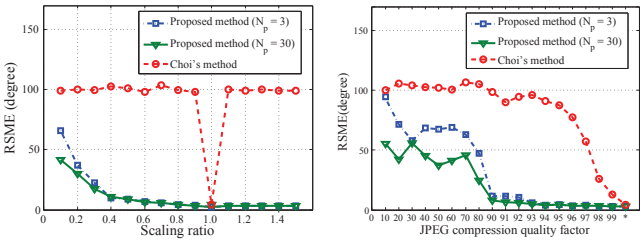


Fig. 6. Estimated RMSE for N_p



(a) (b)

Fig. 7. Estimated RMSE of the degree for (a) image resizing and (b) JPEG compression quality. (* : uncompressed).

4.3. Comparison results with various attacks

The comparison experiments are divided into two parts as follows: image resizing and JPEG compression. The proposed method was performed with $N_p = 3$ and 30. The results of the proposed method were compared to those of Choi's method [2] with interval factor $\Delta s = 1$. We generated reference patterns with images corresponding the type of attacks for suspicious images. This reflects situations in the real-world in which it is difficult to obtain the original image for forgery determination.

4.3.1. Image resizing

Most of the images were resized to a half or less their size because the original images from a digital camera were too large to share on the Internet. Considering the Internet is the main environment for image sharing, robustness to image resizing is a mandatory requirement for forensic schemes.

Fig. 7(a) describes the RMSE values for different image scaling factors. For this experiment, we generated reference patterns with images corresponding to sizes of suspicious images. The results of both methods are qualitatively similar in the case of the scaling ratio 1.0. However, Choi's method did not work with any scaling ratio apart from the original size. On the other hand, the results of the proposed method with a scaling ratio of 0.4 and higher are acceptable.

4.3.2. JPEG compression

JPEG compression is commonly used to compress images in most digital cameras. We compressed the test images by varying the JPEG quality factor from 10 to 100, and tested the proposed method for estimating hue modification. For this experiment, all of the reference patterns were generated by compressed images.

Fig. 7(b) shows the RMSE values for different JPEG compression qualities. The performance of the proposed method for images with a JPEG quality factor upwards of 95 was as sufficient as the case of the uncompressed result. The results in the cases of the quality factor between 80 to 95 were also acceptable.

On the other hand, even with tests with a high JPEG quality factor such as 98 and 97, Choi's method [2] demonstrated relatively poor performance for estimating the hue modification. Under a quality factor of 95, Choi's method did not perform.

5. CONCLUSION

In this paper, we proposed an image forensics method for estimating hue modification using sensor pattern noise. This method achieved robustness to JPEG compression and scaling which were not achieved from a previous method. Our algorithm estimates hue modification of entire area of an image, and we can design an algorithm for estimation of local area by adopting other methods [6–8]. However, the proposed estimation method is testing suspicious images for all hue changes and thus consumes much time. Therefore, we plan to design a search scheme that narrows down the hue modification candidates. We also plan to extend the estimation of other types of image property modification such as white balancing, and saturation.

Acknowlegdement

This research project was supported by Government Fund from Korea Copyright Commission.

6. REFERENCES

[1] "Bild manipulationen : Beispiel farbmanipulation," `http://rhetorik.ch/Bildmanipulation/`, 2011.

[2] Chang-Hee Choi, Hae-Yeoun Lee, and Heung-Kyu Lee, "Estimation of color modification in digital images by CFA pattern change," *Forensic Science International*, vol. 226, pp. 94–105, 2013.

[3] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *Information Forensics and Security, IEEE Transactions on*, vol. 1, no. 2, pp. 205–214, 2006.

[4] J.R. Janesick, *Scientific Charge-coupled Devices*, Press Monographs. Society of Photo Optical, 2001.

[5] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," Feb. 2006, vol. 6072 of *SPIE Conference Series*, pp. 362–372.

[6] Mo Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 1, pp. 74–90, March 2008.

[7] G. Chierchia, S. Parrilli, G. Poggi, L. Verdoliva, and C. Sansone, "Prnu-based detection of small-size image forgeries," in *Digital Signal Processing (DSP), 2011 17th International Conference on*, July 2011, pp. 1–6.

[8] G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, "Prnu-based forgery detection with regularity constraints and global optimization," in *Multimedia Signal Processing (MMSP), 2013 IEEE 15th International Workshop on*, Sept 2013, pp. 236–241.

[9] Nathan Moroney, Mark D. Fairchild, Robert W. G. Hunt, Changjun Li, M. Ronnier Luo, and Todd Newman, "The ciecam02 color appearance model," in *IS&T/SID 10 th Color Imaging Conference*, 2002, pp. 23–27.

[10] Preucil Frank, "Color hue and ink transfer - theri relation to perfect reproduction," in *Proceedings of TAGA*, 1953, pp. 102–110.

[11] Bryce E. Bayer, "Color imaging array," 1976, U.S. Patent 3971065.

[12] Thomas Gloe, Antje Winkler, and Karsten Borowka, "Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics," in *SPIE Conference on Media Forensics and Security*, 2010.

[13] Chuan-kai Lin, "Pixel grouping for color filter array demosaicing," `http://sites.google.com/site/chklin/demosaic`, Apr. 2003.