ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 65, No. 12, pp. 2153~2158, 2016
http://dx.doi.org/10.5370/KIEE.2016.65.12.2153

Wiener 필터링에 기반하는 센서 패턴 노이즈를 활용한 영상 장치 식별 기술 연구

Imaging Device Identification using Sensor Pattern Noise Based on Wiener Filtering

이 해 연*
(Hae-Yeoun Lee)

Abstract - Multimedia such as image, audio, and video is easy to create and distribute with the advance of IT. Since novice uses them for illegal purposes, multimedia forensics are required to protect contents and block illegal usage. This paper presents a multimedia forensic algorithm for video to identify the device used for acquiring unknown video files. First, the way to calculate a sensor pattern noise using Wiener filter (W-SPN) is presented, which comes from the imperfection of photon detectors against light. Then, the way to identify the device is explained after estimating W-SPNs from the reference device and the unknown video. For the experiment, 30 devices including DSLR, compact camera, smartphone, and camcorder are tested and analyzed quantitatively. Based on the results, the presented algorithm can achieve the 96.0% identification accuracy.

Key Words : Multimedia forensics, Sensor patter noise, Imaging device identification, Wiener filter

1. Introduction

Information technology has been rapidly advanced in recent years. As a result, multimedia devices and software can be easily accessed to everyone with low cost, high quality and high performance. Particularly, multimedia devices including imaging sensors such as digital camera, camcorder, smart phone and tablet PC are widely used to create and distribute multimedia contents.

Since novice uses these devices for illegal purposes, many crimes with these devices are increasing and become critical social issues. In the film industry, there has been serious economic loss because of illegal recording and distributing films in a cinema. Also, there have been many sexual crimes using spy camera or smart phone with secret camcording. In most crimes, images or videos from CCTV and car black box are referred to solve cases. Also, they are adopted as evidences in many courts.

However, multimedia such as images, audios, and videos are exposed to forgery and that can cause serious social and legal problems. Therefore, a technique to protect the illegal usage of multimedia is required and multimedia forensics can be an effective solution to protect contents and block illegal usage. Moreover, social and economic needs for multimedia forensic techniques will be increased with increasing of crimes using multimedia contents.

Images and videos acquired using imaging devices contain a unique noise characteristics because of the imperfection of photon detectors in the production process. Therefore, this unique noise characteristics can be used as a fingerprint for each imaging device.

In this paper, a multimedia forensic algorithm for video files is presented to identify the imaging device that is used for acquiring the video files. First, the way to acquire a sensor pattern noise using Wiener filter (W-SPN) is presented, which can be a unique noise characteristics of photon detectors. Then, the way to identify the imaging device is explained after estimating W-SPNs from the reference device and the unknown video. The presented algorithm is tested on 30 devices and achieved the 96.0% identification accuracy

The paper is organized as follows. Section 2 reviews multimedia forensics techniques. An imaging device identification algorithm is proposed in Sec. 3. Experimental results are presented in Sec. 4 and Section 5 concludes.

2. Related Works

The technique to identify imaging devices is similar to find guns that have fired a bullet through the analysis of

* Corresponding Author : Dept. of Computer Software Engineering, Kumoh National Institute of Technology, South Korea.
E-mail: haeyeoun.lee@kumoh.ac.kr
Received : October 13, 2016; Accepted : November 17, 2016

patterns or traces of gun barrels remaining in the bullet during criminal investigation.

In multimedia forensic techniques, the way to extract accurately the unique feature that is embedded in the contents is critical for the performance. The extracted unique features can be used for source identification or forgery detection.

Fridrich et al. identified imaging cameras by extracting the photo response non-uniformity (PRNU) of imaging sensors, which is unintentionally caused during the imaging process [1, 2]. Since color filter array (CFA) is adopted in most imaging devices, Memon et al. performed researches to identify the imaging device by considering interpolation artifacts from CFA [3]. Hyun et al. studied a technique to identify CCTV by analyzing sensor pattern noise from CCTV videos [4].

Farid et al. developed a technique to identify the forgery of contents using camera skewness parameters which come from the space-time correlation of images or analyzing the statistical properties of video compression formats [5, 6]. Choi et al. studied a technique to detect image forgery where the change of interpolated artifacts from CFA is detected [7].

Multimedia forensics for source identification have a tendency to use PRNU steadily. Multimedia forensics for forgery detection have been continuously studied to find the stationery statistical properties of images and videos [8].

2.1 Video Acquisition and Sensor Pattern Noise

Most general-purpose imaging devices have an image acquisition process as depicted in Fig. 1. The light from the object passes through the lens of the equipment. Then, it passes through the anti-aliasing filter and reaches the sensor through the color filter array (or matrix). The photon detector in the sensor measures the amount of light incident. Since the sensor measures the light in accordance with the arrangement of the CFA (red, green, blue channels), each light of channel is de-mosaicked and post-processed to make the image or frame.

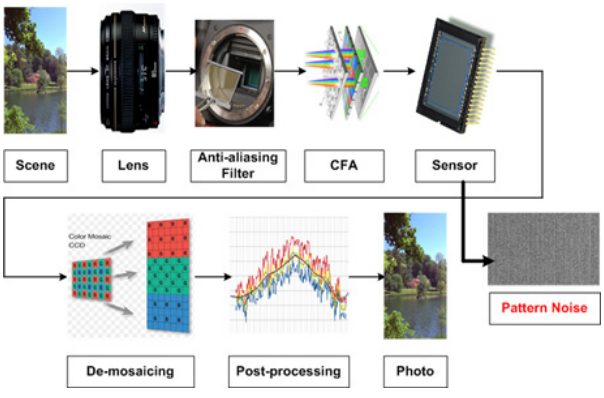

Fig. 1 Image acquisition process of imaging devices

Most imaging devices have a sensor and hence can be identified by the uniqueness of pattern noise. A way to extract sensor pattern noise is the use of fixed pattern noise (FPN). FPN is equivalent to dark currents caused by thermal reasons without light. However, FPN is not acceptable for identifying imaging devices because it is measured only in a limited condition.

A variety of imaging devices such as digital camera, smart phones, camcorders, and scanner use an imaging sensor such as CCD or CMOS. This sensor is composed of an array of many photon detectors, which convert detected photons into electrical signals by the photo-electric effect. The intensity of the electric signals is determined by the sensitivity to the light of photon detectors.

However, each photon detector has imperfectness during the production. For this reason, imaging devices have a unique sensor pattern noise (SPN). This non-uniformity can be used as a measure of the inherent characteristics of sensors. The way to extract Wiener filter-based SPN used in this paper will be described in Sec. 3.1.

3. Proposed Imaging Device Identification Algorithm

For video files, there is a unique embedded noise which is inherent from the imaging sensor. By identifying this embedded noise, the sensor acquiring the video files can be identified.

The overall process to identify the imaging device is depicted in Fig. 2. For the reference frames from camcorder, Wiener filter-based sensor pattern noise(W-SPN) is calculated by extracting noise with Wiener filter, averaging the extracted noise and removing frequent artifacts. Similarly the W-SPN of test frames from an unknown video file is calculated. Then, by calculating correlation between two W-SPNs, decision can be made whether the unknown video is acquired by the reference camcorder.

The way to extract the W-SPN is explained in Sec. 3.1. The way to identify the similarity between two W-SPNs is presented in Sec. 3.2.

3.1 Wiener filter-based Sensor Pattern Noise Extraction

As the unique characteristics of imaging sensors, photo response non-uniformity based on Wiener filter is extracted which is called as Wiener filter-based sensor pattern noise (W-SPN).

The intensity I of a frame can be modeled as follows.

$$I = g^r \cdot \left[(1+K)Y + \Lambda\right]^r + Q \tag{1}$$

Y is the indirect light from the object. g is each color channel gain, r is gamma correction coefficient, K is a sensor pattern noise, Λ is a combination of independent noise, and Q is quantization and compressed noise.

The way to extract W-SPNs, K', from reference frames of M video files is composed of 2 steps. In the first step, noises from each frame are extracted by applying Wiener filter and then all extracted noises are averaged as follows.

$$K = \sum_{i=1}^{M}\left(\sum_{k=1}^{N} W_{i,k} I_{i,k} \Big/ \sum_{k=1}^{N} {I_{i,k}}^2\right) \tag{2}$$

where $W = I - WF(I)$, WF is Wiener filter, N is the number of frames in each video.

Since the averaged noise in the first step is the estimation of W-SPN for general images, its accuracy is low because of block effects from 8x8 block or macro-block during MPEG compression. In the second step, since these effects have periodic characteristics, Fourier transform is performed and Wiener filtering is applied to remove these block effects and noises as follows.

$$K' = F^{-1}\left\{F(K) - W(F(K))\right\} \tag{3}$$

where F is Fourier transform and W is Wiener filtering. The W-SPN is K'.

The W-SPN, T', can be extracted from the test frames of the unknown video in similarly to the W-SPN of reference videos. However, only 1 video is considered as follows.

$$T = \sum_{k=1}^{N} W_{i,k} I_{i,k} \Big/ \sum_{k=1}^{N} {I_{i,k}}^2 \tag{4}$$

$$T' = F^{-1}\left\{F(T) - W(F(T))\right\} \tag{5}$$

For the W-SPNs of reference camcorder, noise is extracted from frames taken to have constant brightness and uniform dispersion and then averaged for the stability, which will remain W-SPN and remove other noises.

Fig. 3 depicts W-SPN examples extracted from 30 frames of videos using imaging sensors. Since the W-SPN is the estimation of the actual sensor pattern noise, there exist effects from contents, which can be minimized by averaging many frames.

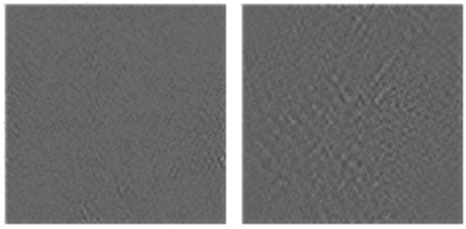

Fig. 3 Example of W-SPN from 30 frames

3.2 Similarity Identification

In Sec. 3.1, the W-SPN, K', from the reference camcorder and the W-SPN, T', from the unknown video are calculated. In order to determine whether the unknown video is acquired from the reference camcorder, the similarity is measured.

As a similarity measure, normalized correlation coefficient (NCC) is calculated as follows.

$$NCC(K', T') = \frac{(K' - \overline{K}') \cdot (T' - \overline{T}')}{\left\|K' - \overline{K}'\right\| \left\|T' - \overline{T}'\right\|} \tag{6}$$

When the calculated NCC is greater than a threshold, it can be identified that the unknown video is acquired using the reference camcorder. If not, the unknown video is not acquired using the reference camcorder.

$$Identification = \begin{cases} match & if \;\; NCC(K', T') \geq threshold \\ no - match & otherwise \end{cases} \tag{7}$$

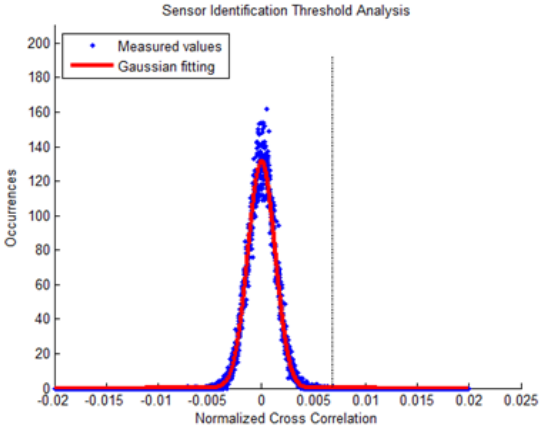

Fig. 4 NCC distribution and Gaussian fitting model when reference and unknown videos are not matched

About 1,305,000 frames, Fig. 4 depicts the distribution of the measured NCC when the reference W-SPNs and the test W-SPNs from unknown videos are not matched. NCC distribution follows a Gaussian distribution, whose center is 0 indicating no similarity. Therefore, this distribution is fit as Gaussian model and the threshold is calculated depending on the probability. When error probability is set at 1/1,000,000, the threshold is 0.0068 which is used in our experiment.

4. Experimental Results

4.1 Experimental Setup

30 imaging devices from 13 brands as shown in Table 1 are considered to analyze the performance of the algorithm.

Table 1. Device lists for performance analysis

Brand	Model	Resolution	FPS
Canon	EOS 650D	1920x1088	25
	EOS 500D	1920x1088	20
	EOS M	1280x720	50
	EOS M3	1280x720	25
	IXUS 160	1920x1080	29
Nikon	Coolpix S100	1920x1080	29
	Coolpix S33	1920x1080	29
Panasonic	Lumix DMC SZ1	1280x720	29
	Lumix DWC LX100	3840x2160	29
Olympus	PEN Mini	1280x720	30
Samsung	WB35F	1280x720	30
	NX Mini	1920x1080	25
Sony	HDR XR520	1440x1080	29
Samsung	Galaxy Note3	1920x1080	29
GoPro	GoPro Hero4	1920x1080	29
LG	G2	1920x1080	21
	G3 Cat6	1920x1080	29
	G4	1920x1080	29
	Vu3	1440x1080	29
Samsung	Galaxy Grand Max	1920x1080	29
	Galaxy Note2	1920x1080	29
	Galaxy Note2	1920x1080	30
	Galaxy Note4	1920x1080	29
	Galaxy S4	1920x1080	30
	Galaxy S5	1920x1080	29
	Galaxy Zoom2	1920x1080	30
Huawei	P8 GRA UL00	1280x720	29
Shaomi	MI Note LET	1280x720	29
Apple	iPhone 6plus	1920x1080	30
Pantech	Vega Secret Note	1920x1080	29

Without any special setting for each device, 5 videos about 10 seconds were taken to estimate the reference W-SPNs of the reference devices. 5 videos about 10 seconds were taken for testing identification accuracy. Therefore, 300 video files were utilized for analysis. Since each video has more than 300 frames, about 90,000 frames are processed. Also, since the size of videos are different from, 1024x1024 region in the center is cropped and used.

Since video files are compressed in MPEG standard, W-SPN will be damaged. However, the algorithm should resist against this compression for the practical usage.

In case of reference videos, blue or cloudy sky are taken to get uniform brightness without special objects. In case of test videos, natural scenes are taken and we have tried to take the same objects for each video in order to minimize

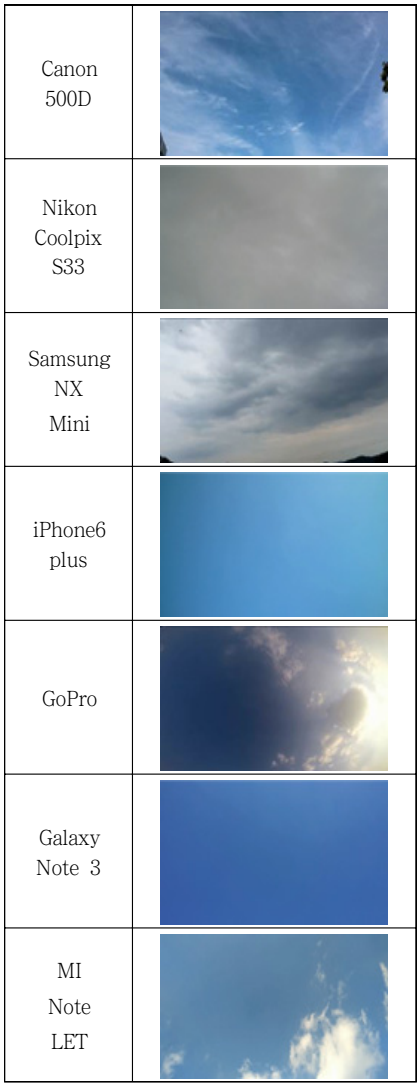

Fig. 5 Samples of reference frames for each device

the performance difference depending on the objects as shown in Fig. 5 and 6.

4.2 Identification Accuracy

To analyze the identification accuracy of the proposed imaging device identification algorithm, we performed intensive testing. After W-SPNs are extracted from 5 reference videos from 30 devices, W-SPNs from unknown videos from 30 devices are extracted and the similarity between these W-SPNs is measured by comparing normalized correlation coefficient. Then, the device having the high NCC is considered that the unknown video is acquired by that device.

For 150 test videos from 30 devices, source identification rate is summarized in Fig. 7. Except several devices such as

Fig. 6 Samples of testing frames for each device

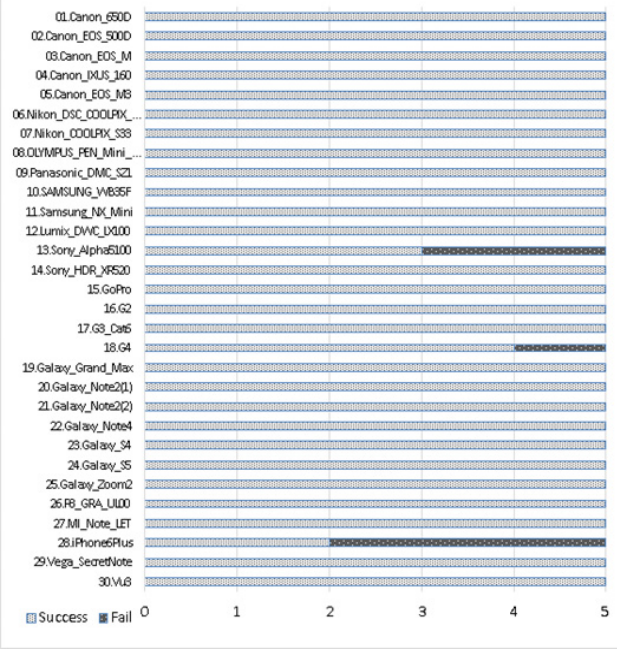

Fig. 7 Imaging device identification result.

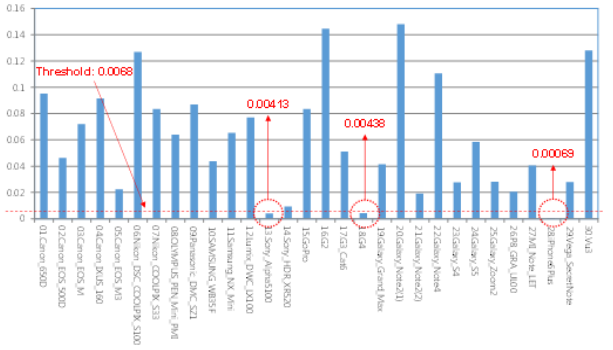

Fig. 8 Device identification accuracy for each device

Sony Alpha 5100, LG G4 and iPhone6 plus, all test videos are correctly identified. The average identification rate for 30 devices was 96.0%. As shown in Fig. 8, the similarity of some videos from Sony Alpha 5100, LG G4 and iPhone6 plus was under the threshold, 0.0068, of error probability 1/1,000,000. However, the similarity value of these identification failure videos was relatively high at the exact device over other devices.

5. Conclusion

Multimedia is easy to create and distribute with the advance of IT. However, novices use them for illegal purposes and raise serious crimes. Therefore, multimedia

forensic techniques are inevitable.

In this paper, a source identification algorithm for video files is presented using Wiener filter-based sensor pattern noise. The way to extract W-SPN from the reference device and W-SPN from the unknown video was presented. Also, the way to calculate the similarity for identification was presented. To show the performance, intensive tests were performed by considering 30 devices from 13 brands and results confirmed that the presented algorithm could perform well.

This algorithm can be used for various applications. It can identify illegal content manufacturers. Also, it can check the integrity of security contents from CCTV and car black box. It can be applied for copyright protection. Differently from digital watermarking that modifies contents, multimedia forensics can be applied without any modification of contents and hence there will be many applications.

Acknowledgement

This work was supported by the research fund of National Security Research Institute (2016-082)

References

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

[2] M. Chen, J. Fridrich, and M. Goljan, "Source digital camcorder identification using ccd photo response non-uniformity," Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, pp. 1G-1H, 2007.

[3] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas "Source Camera Identification Based on CFA Interpolation," Proceedings of IEEE Int. Conf. on Image Processing (ICIP), pp. 69-72, 2005.

[4] D.-K. Hyun, S.-J. Ryu, H.-Y. Lee, and H.-K. Lee, "Detection of Upscale-Crop and Partial Manipulation in Surveillance Video based on Sensor Pattern Noise," Sensors, vol. 13, no. 9, pp. 12605-12631, Sep. 2013.

[5] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling," IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 758-767, Feb. 2005.

[6] W. Wang and H. Farid, "Exposing Digital Forgeries in Video by Detecting Double MPEG Compression," Proceedings of the 8th workshop on ACM Multimedia and security, pp. 37-47, 2006.

[7] C. H. Choi, H.-Y. Lee, and H.-K. Lee, "Estimation of Color Modification in Digital Images by CFA Pattern Change," Forensic Science International, vol. 226, no. 1-3, pp. 94-105, March 2013.

[8] C.-T. Li, "Source Camera Identification Using Enhanced Sensor Pattern Noise," IEEE Transactions on Information Forensics Security, vol. 5, no. 2, pp. 280-287, June 2010.

저 자 소 개

Hae-Yeoun Lee

Hae-Yeoun Lee received his MS and PhD degrees in computer science from Korea Advanced Institute of Science and Technology (KAIST) in 1997 and 2006, respectively. From 2001 to 2006, he was with Satrec Initiative, Korea. From 2006 to 2007, he was a postdoctoral researcher at Weill Medical College, Cornell University, United States. He is now with Kumoh National Institute of Technology, Korea. His major interests are image processing, digital watermarking, digital forensics, remote sensing, and digital rights management.