Morphology-Based Sensor Pattern Noise Extraction for Device Identification

Hae-Yeoun Lee
Department of Computer Software Engineering, Kumoh National Institute of Technology, 61 Daehak-ro, Gumi, Gyeongbuk, Republic of Korea
Email: haeyeoun.lee@kumoh.ac.kr

***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. Using a Morphology-based Sensor Pattern Noise (M-SPN), 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 morphology filter is presented, which comes from the imperfection of photon detectors against light. Then, the way to identify the device is explained after estimating M-SPNs from the reference device and the unknown video. For the experiment, 15 devices including DSLR, compact camera, smartphone, and camcorder are tested and analyzed quantitatively. Based on the results, the presented algorithm can achieve the 92.0% identification accuracy.**

***Index Terms*—multimedia forensics, sensor pattern noise, imaging device identification, morphology filter**

I. 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 a 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 an evidence 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 morphology filter (M-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 M-SPNs from the reference device and the unknown video. The presented algorithm is tested on 15 devices and achieved the 92.0% identification accuracy

The paper is organized as follows. Section II reviews multimedia forensics techniques. A device identification algorithm is proposed in Section III. Experimental results are presented in Section IV and Section V concludes.

II. Related Works

As shown in Fig. 1, the technique to identify imaging devices is similar to find guns that have fired a bullet through the analysis of patterns or traces of gun barrels remaining in the bullet during criminal investigation.

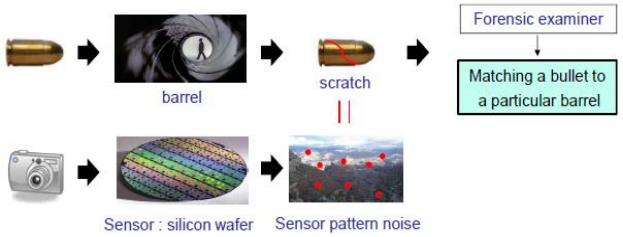

Figure 1. Basic idea of device identification technique

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)

Manuscript received April 19, 2016; revised August 12, 2016.

doi: 10.18178/joig.4.2.145-149

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 studied to find the stationery statistical properties of images and videos [8].

A. Video Acquisition and Sensor Pattern Noise

Most general-purpose imaging devices have an image acquisition process. 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 [9].

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 [10].

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 morphology-based SPN will be described in Section III.A.

III. Morphology-Based Sensor Pattern Noise Extraction for Device Identification

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, Morphology-based Sensor Pattern Noise (M-SPN) is calculated by extracting noise with morphological operation, averaging the extracted noise and removing frequent artifacts. Similarly the M-SPN of test frames from an unknown video file is calculated. Then, by calculating correlation between two M-SPNs, decision can be made whether the unknown video is acquired by the reference camcorder.

The way to extract the M-SPN is explained in Section III.A. The way to identify the similarity between two M-SPNs is presented in Section III.B.

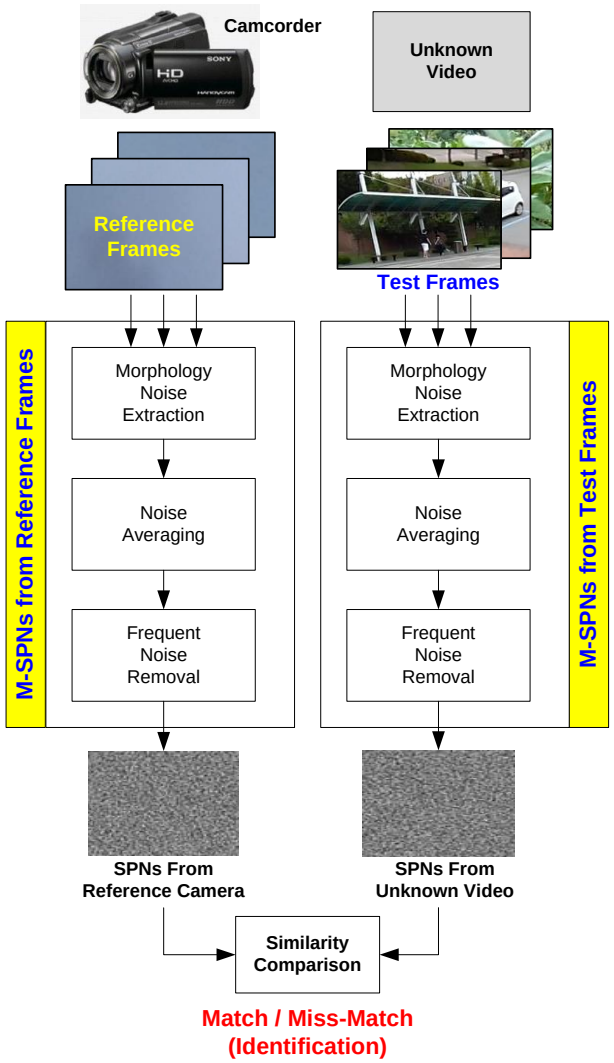

Figure 2. Proposed imaging device identification process

A. Morphology-Based Sensor Pattern Noise Extraction

Morphology in image processing is a collection of non-linear operations related to the morphology of features in images. Although morphological operations are applied to binary images, they can be applied to grayscale images, where the structuring elements for grayscale morphology are real-valued 2D functions. A representative morphological operations is erosion and dilation. Erosion in grayscale images is the minimum of the difference values between structuring elements and their overlaid pixels. Dilation in grayscale images is the maximum of the added values. Similarly to binary images, opening is applying dilation after erosion and closing is

applying erosion after dilation. In this research, opening in morphological operations is applied to get noisy features in grayscale images [11].

For the device identification, photo response non-uniformity based on morphology filter is extracted and used as the unique characteristics of imaging sensors, which is called as Morphology-based sensor pattern noise (M-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 M-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 morphological 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 $W = I - MF(I)$, MF is morphological filter, N is the number of frames in each video.

Since averaged noises in the first step are the estimation of M-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 morphological 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 M-SPN is K'.

The M-SPN, T', can be extracted from the test frames of the unknown video in similarly to the M-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 M-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 remains M-SPN and removes other noises.

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

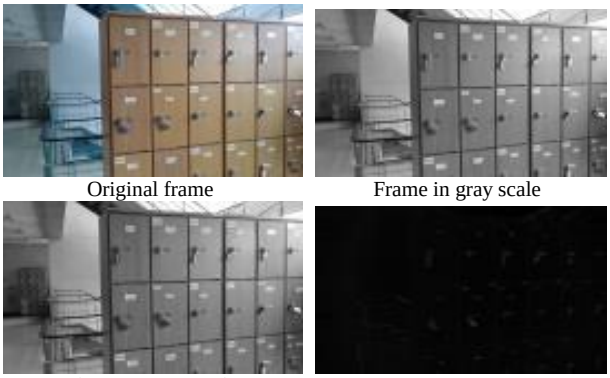

Figure 3. Example of M-SPN with morphology filtering

B. Similarity Identification

In Section III.A, the M-SPN, K', from the reference camcorder and the M-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 [12].

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

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.

About 1,305,000 frames, Fig. 4 depicts the distribution of the measured NCC when the reference M-SPNs and the test M-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 0.0083 which is used in our experiment.

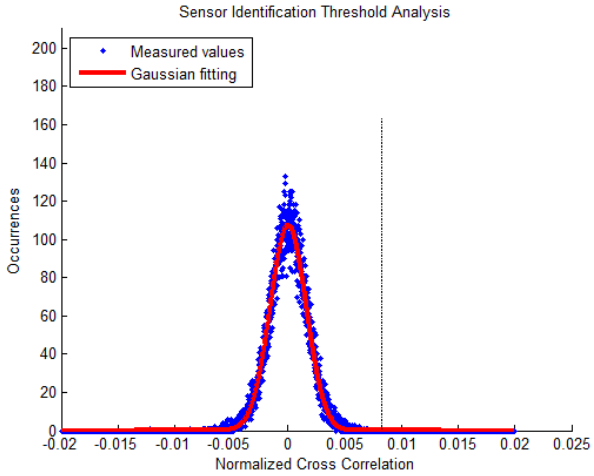

Figure 4. NCC distribution and Gaussian fitting model when reference and unknown videos are not matched

IV. Experimental Results

15 imaging devices from 8 brands as shown in Table I are considered to analyze the performance of the algorithm. As shown in Fig. 5, without any special setting for each device, 5 videos about 10 seconds were taken to estimate the reference M-SPNs of the reference devices. 5 videos about 10 seconds were taken for testing identification accuracy.

TABLE I. Device Lists for Performance Analysis

Brand	Model	Resolution	FPS
Canon	EOS 650D	1920x1088	25
	EOS 500D	1920x1088	20
	EOS M	1280x720	50
Nikon	Coolpix S33	1920x1080	29
Olympus	PEN Mini	1280x720	30
Samsung	NX Mini	1920x1080	25
	Galaxy Grand Max	1920x1080	29
	Galaxy Note4	1920x1080	29
	Galaxy Zoom2	1920x1080	30
Gopro	GoPro Hero4	1920x1080	29
LG	G2	1920x1080	21
	G3 Cat6	1920x1080	29
	Vu3	1440x1080	29
Shaomi	MI Note LET	1280x720	29
Apple	iPhone 6plus	1920x1080	30

Figure 5. Samples of reference and testing frames for each device

Therefore, 150 video files were utilized for analysis. Since each video has more than 300 frames, about 45,000 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, M-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 the performance difference depending on the objects as shown in Fig. 5.

A. Identification Accuracy

To analyze the identification accuracy of the proposed imaging device identification algorithm, we performed intensive testing. After M-SPNs are extracted from 5 reference videos from 15 devices, M-SPNs from unknown videos from 15 devices are extracted and the similarity between these M-SPNs are 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 75 test videos from 15 devices, source identification rate and accuracy are summarized in Fig. 6 and Fig. 7. Except several devices such as Canon EOS 500D, Olympus Pen Mini, and iPhone 6 plus, all test videos are correctly identified. The average identification rate for 15 devices was 92.0%. The similarity of some videos from Canon EOS 500D and Olympus Pen Mini was under the threshold, 0.0083, 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.

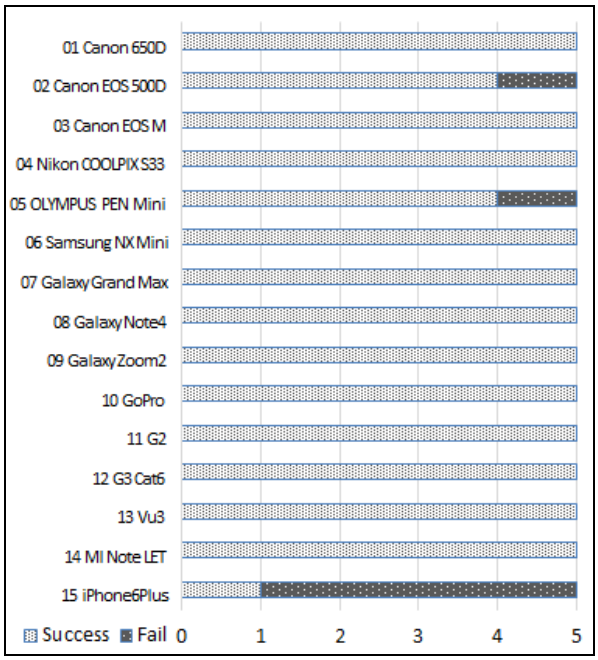

Figure 6. Imaging device identification result

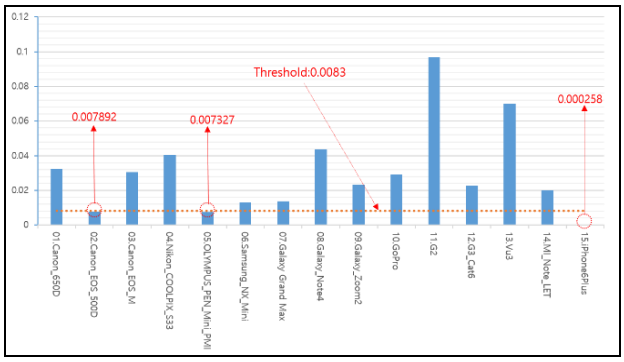

Figure 7. Device identification accuracy for each device

V. Conclusion

Multimedia is easy to create and distribute with the advance of Information Technology. However, novices use them for illegal purposes and raise serious crimes in these days. Therefore, multimedia forensic techniques are inevitable.

In this paper, a device identification algorithm for video files is presented using morphology-based sensor pattern noise. The way to extract M-SPNs from the reference device and M-SPNs from the unknown video was presented using morphological filtering. Also, the way to calculate the similarity for identification was presented. To show the performance, intensive tests were performed using 15 devices from 8 brands and experimental 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.

Acknowledgment

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," in *Proc. SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, 2007, pp. 1G–1H.

[3] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, "Source camera identification based on CFA interpolation," in *Proc. IEEE International Conference on Image Processing*, 2005, pp. 69–72.

[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," in *Proc. 8th Workshop on ACM Multimedia and Security*, 2006, pp. 37-47.

[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, An International Journal*, vol. 226, no. 1-3, pp. 94-105, Mar. 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.

[9] W. Lu and Y. P. Tan, "Color filter array demosaicking: New method and performance measures," *IEEE Transactions on Image Processing*, vol. 12, no. 10, pp. 1194-1210, Sep. 2003.

[10] P. Magnan, "Detection of visible photons in CCD and CMOS: A comparative view," in *Proc. 3rd International Conference on New Developments in Photodetection*, vol. 504, no. 1-3, pp. 199-212, May 2003.

[11] E. R. Dougherty and R. A. Lotufo, *Hands-on Morphological Image Processing*, SPIE Press, 2003, pp. 91-125.

[12] H. Y. Lee, H. Kim, and H. K. Lee, "Robust image watermarking using local invariant features," *Optical Engineering*, vol. 45, no. 3, pp. 1-11, Mar. 2006.

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.