# Optimized Digital Library for Digital Forenisc Based on Decomposed PRNU

Yue Li
College of Software
Nankai University
Tianjin, China
liyue80@nankai.edu.cn

Chang-Tsun Li
Department of Computer Science,
University of Warwick,
Coventry, UK
c-t.li@warwick.ac.uk

***Abstract*—Nowadays, the digital forensic techniques for digital images are developed with the origin identification and integrity verification functions for security reasons. Methods based on photo-response-non-uniform (PRNU) are widely studied and proved to be effective to serve the forensic purposes. However, due to the interpolation noise, caused by the colour filtering and interpolation function the accuracy of the PRNU-based forensic method has been degraded. Meanwhile, the tremendous physical storage requirement and computation consumption limit the applications of PRNU-based method. Therefore, an innovative DPRNU-based forensic method has been proposed in order to solve the above problems. In the method, the artificial component and physical component are separated according to the colour filtering array (CFA) and the PRNU are only extracted from the physical component in order to remove the interference caused by the interpolation noise, which increases the accuracy of the camera identification and integrity verification. Meanwhile, due to the separation, the DPRNU are only 1/3 of the size of the traditional PRNU, which saves considerable physical storage in setting up the digital library and fasters the comparison speed between the fingerprints.**

***Keywords-Forensics, colour filtering array, photo response non-uniformity, digital library***

## I. INTRODUCTION

Nowadays, the widely applied digital imaging devices bring great convince to the people in daily life. At any time, people can capture scenes around them by the portable cameras or the built-in camera in the mobile; the government can achieve 24-hour surveillance by the widely installed CCTV; the journalists can records the 1/24-second-motions by the professional camera. However, the security of the captured digital images remains unprotected and such problem needs urgently investigation by the research and the engineer [1]. As a result, the digital forensic techniques for digital images are developed with the origin identification and integrity verification functions in order to solve the security problems.

Generally speaking, the forensic techniques extract a fingerprint, which is a digital feature left by the digital imaging device, and compared it to the reference fingerprints representing a set of imaging devices in the database [2-5]. Depending on the comparing result, the forensic techniques can identify the origin and verify the integrity of the digital images [1]. Due to the necessity of the reference fingerprint, setting up a digital library, which stores the majority reference fingerprints of the digital devices for comparison, is essential to serve the forensic purposes [6-7]. However, in setting up such digital library, the user may face the serious problem in the physical storage requirement and tremendous time consuming in the computation. In this paper, we will propose a Decomposed PRNU (DPRNU) fingerprint extraction algorithm and set up a digital library based on DPRNU, achieving higher efficiency on time and physical storage.

## II. REVIEW OF THE FORENSIC TECHNIQUES

### *A. Forensic Techniques based on PRNU*

Photo-response-non-uniform (PRNU) is the content-dependent high-frequency noise, which is caused by the imperfections of the sensors during the manufacturing[1]. Because the imperfections are unique to every single sensor and thus to every camera, forensic techniques based on the PRNU are accuracy enough to identify the unique camera. However, the techniques based on PRNU also cause higher computation load.

In acquiring an image, the signals will inevitably be distorted when passing through each process and these distortions result in slight differences between the scene and the camera-captured image [6]. Such distortions can be mathematically described as an additive noise to the signals, and hence the general expression of captured images is

$$I = Y + N \tag{1}$$

where $I$ is the captured image, $Y$ is the perfect representation of the scene and $N$ is the additive noise representing the distortions.

With this additive noise, even if the camera takes pictures of the same scene, the resulting digital images will still exhibit slight differences [6,7]. This is partly because of the *shot* noise (also known as photonic noise), which is a random component uniquely produced in every acquisition process, and partly because of the *pattern noise*, which is a deterministic component that remains the same in pictures of the same scene taken by the same camera. Due to this property, the pattern noise can be utilised as a camera fingerprint for photo authentication.

978-1-61284-774-0/11/$26.00 ©2011 IEEE

### *B. Drawbacks of the Method based on PRNU*

While setting up a digital library for PRNU fingerprint, the users must face two challenges, as the degraded accuracy due to the interpolation noise and the heavy burden to the data storage and computation load.

#### *1) The degraded accuracy due to the interpolation noise*

According to the traditional definition, the sensor pattern noise is the dominant part of the PRNU[6,7]. However, the color filtering and interpolation operation are both important processes but the effect of these operations are not considered. In the filtering, only one color component of every pixel is captured by the sensor, while the other two color components are generated by the interpolation functions for economical reasons. In this work, the color components captured by the sensor are called *physical* components, while the color components generated by the interpolation function are called *artificial* components. According to the CFA working process[8], only one third of the color components of the pixels in the photo are physical components, which contain the sensor pattern noise, while the other two thirds of the color components are artificial components and therefore, the majority of the noise extracted from these component are subsequently the interpolation noise [5]. However, the interpolation noise is extracted but not filtered in the PRNU fingerprint. As discussed in [6,7] such inclusion may lead to interference between the sensor pattern noise and the interpolation noise so that the accuracy of the forensic result will be consequently degraded. As a result, filtering the interpolation noise from the PRNU is necessary to increase the accuracy of the forensic method.

#### *2) Heavy burden to the data storage and computation load*

In the digital library of PRNU, each PRNU represents a camera and therefore, the number of the fingerprint is determined the number of the camera need to be included in the database. Regarding to the huge amount of portable cameras, built-in cameras in the mobile, CCTV cameras and etc, the library of the PRNU will cost tremendous physical storage, which is a great challenge in setting up a fingerprint library[1]. On the other hand, identifying PRNU fingerprints from the database need exhaustive comparisons, which consume considerable computation time. As a result, a method can decrease the digital library size and increase the comparison speed is in need to improve the applicability of this kind of forensic method.

## III. Decomposed PRNU-based forensic method

In this section, an innovative method based on the Decomposed PRNU (DPRNU) has been proposed. In this method, first the CFA is determined by the method proposed by [2], then the pattern corresponds to the physical components are obtained and the PRNU is extracted from these patterns of physical component in order to remove the interpolation noise. The details of this algorithm are presented in the following of this section.

To extract the DPRNU, we first separate the three color channels $I_c$, $c \in \{R,G,B\}$ of a color image $I$ of $X \times Y$ pixels. Most CFAs are of 2 × 2 pixels and are repeatedly mapped to the sensors. We know that, for each pixel of $I$, only one of the three color components is physical and the other two are artificial, so the second step is, for each channel $I_c$, we perform 2:1 down-sampling across both horizontal and vertical dimensions to get four sub-images, $I_{c,i,j}$, where $i$ and $i,j \in \{0,1\}$, such that

$$I_{c,i,j}(x,y) = I_c(2x+i, 2y+j) \qquad (2)$$

where $x \in [0, \lfloor X/2 \rfloor - 1]$ and $y \in [0, \lfloor Y/2 \rfloor - 1]$.

Then applying the CFA estimation algorithm, developed in [5], we can determine the employed CFA in the camera, and seek out the certain $(i,j)$ pairs which satisfies that the sub-image $I_{c,i,j}$ only consist of the physical component but does not contains any artificial components. For example, in an image filtered by the Bayer CFA, $I_{R,0,0}$, $I_{G,0,1}$, $I_{G,1,0}$ and $I_{B,1,1}$ are the sub-images containing physical components. PRNU noise pattern, $P_{R,0,0}$, $P_{G,0,1}$, $P_{G,1,0}$ and $P_{B,1,1}$, extracted from these sub-images using the method in [6], are the noise pattern contains majority sensor noise and no interpolation noise. By decoupling the physical and virtual colour components in the fashion before extracting the PRNU noise pattern, we can prevent the interference error of the artificial components from contaminating the physical components during the DWT process. The wavelet-based denoising process, i.e., a DWT followed by a Wiener filtering operation [6] are used to obtain the PRNU noise patterns $P_{c,i,j}$.

Table 1: DPRNU extraction algorithm.

*Input*: original image $I$

*Output*: DPRNU pattern noise $P$

***DPRNU extraction algorithm***

1) Decompose image $I$ into $R$, $G$, and $B$ components, $I_R$, $I_G$, and $I_B$, respectively.
2) $\forall c \in \{R,G,B\}$, decompose $I_c$ into four sub-images, $I_{c,1,1}$, $I_{c,1,2}$, $I_{c,2,1}$ and $I_{c,2,2}$ by using Equation (2) .
3) $\forall c \in \{R,G,B\}$, $P_{c,i,j}$, $i,j = 1,2$ are obtained by denoising the sub-images $I_{c,i,j}$, using the Wiener filtering in the DWT domain [1]
4) $\forall c \in \{R,G,B\}$, generate the DPRNU, $P_c$ by combining $P_{c,1,1}$ to $P_{c,2,2}$ following Equation (3)
5) Combine the DPRNU noise pattern $P_R$, $P_G$, $P_B$ to form the final DPRNU noise pattern $P$.

Meanwhile, the finally the DPRNU $P$ is represented by the four noise pattern extracted from the sub-images of physical components

$$P=\left\{P_{c,i,j}\right\}, \text{where } P_{c,i,j} \text{ is extracted from } I_{c,i,j} \text{ of physical components} \quad (3)$$

According to the definition of CFA, only 1/3 of the components are captured by the sensor and recorded as physical components, and hence, the final DPRNU only contains 1/3 of the noise pattern of the original PRNU fingerprint. The the procedures are listed in Table 1.

## IV. EXPERIMENT RESULTS

In this section, we carry out experiments in order to prove that 1) the DPRNU outperform the traditional PRNU in source camera identification and image content verification; 2) DPRNU save up the physical storage in setting up the digital library and increase the computing speed. In the experiments of source camera identification, we will trace the source cameras of digital photos by comparing the extracted DPRNU with the reference DPRNU of the cameras. In the experiments of image content verification, we can detect forged area by investigating the integrity of the DPRNU.

### *A. Camera Identification*

To demonstrate the performance of the proposed DPRNU, we have carried out identification tests on 300 2048×1536-pixel photos of natural scenes taken by six cameras, each responsible for 50. The six cameras are listed in Table 2.

TABLE I. : CAMERA LIST.

| **Symbol** | $C_1$ | $C_2$ | $C_3$ |
|---|---|---|---|
| Camera | Canon IXUS 850IS | Canon PowerShot A400 | Canon IXY Digital 500 |
| **Symbol** | $C_4$ | *C5* | *C6* |
| Camera | FujiFilm A602 | Olympus FE210 | Olympus C730 |

Each reference PRNU (i.e., $r_d$ ), that represents one camera, is generated according to Equation in [1], which calculates the element-wise weighted average of the PRNUs extracted from 30 photos of blue sky taken by the digital camera. Source camera identification requires similarity comparisons among PRNUs (DPRNUs) and therefore the feasibility of the chosen similarity metrics is important. In the following experiments, cross-correlation as formulated in Equation (4) will be used to measure the similarity between PRNUs (DPRNUs). In this experiment, the key point is about demonstrating the different performance of the traditional PRNU and the proposed DPRNU. Therefore, a camera is identified as the source camera, if out of the six reference PRNU (or DPRNU), its reference PRNU (or DPRNU) is most similar to the PRNU (or DPRNU), $n_I$, of the image, $I$, under investigation. That is to say, camera $C_i$, $i \in [1,6]$ is identified as the source camera if

$$d = \arg\max_i \left( \left\{ \rho\left(n_I, I \cdot r_i\right) \middle| i \in [1,6] \right\} \right) \quad (4)$$

Due to the length limitation, we only list the ROC curve on average detection rate for DPRNU and PRNU, in Figure 1. In this figure, the DPRNU outperforms the PRNU in the origin detection.

### *B. Content Integrity Verification*

To demonstrate the performance of the proposed DPRNU, we carry out integrity verification experiments on one $640\times480$-pixel images taken by Olympus C730 ($C_6$ in Table 2 of the camera list). In the experiments, we cut off an $640\times480$-pixel area from image in Figure 2(a), paste an area copied from a different location in the in Figure 2 (b) to create the forged (c). The PRNUs in the two areas are different due to the different locations, though both Figure 2 (a) and Figure 2 (b) are captured by the camera $C_6$.

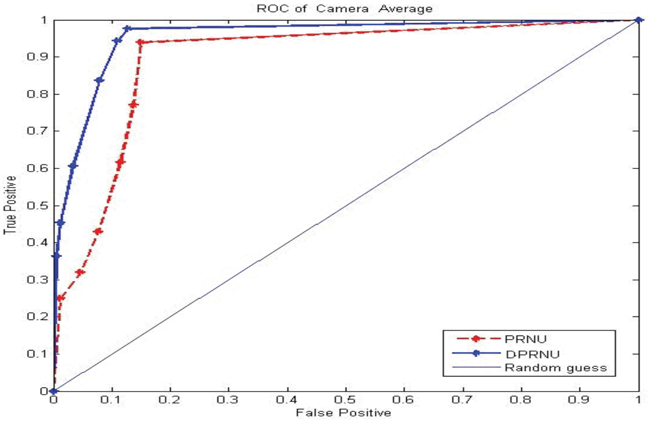

Figure 1. Overall ROC curve for DPRNU and PRNU in origin identification

To detect the manipulated areas, we create two $128\times128$-pixel sliding windows and one window is moved across the PRNU extracted form the image under investigation, whilst the other window is moved across the reference PRNU of the cameras. The cross-correlation of the two PRNU pattern inside the two windows is calculated, and if the cross-correlation is lower than a predetermined threshold, the pixel in the centre of the window is deemed to be forged. In our experiment, the sliding step/displacement is 5 pixels. In the image, there are totally 358 blocks manipulated and 7130 blocks non-manipulated blocks in the size of $5\times5$ pixels in the forged images.

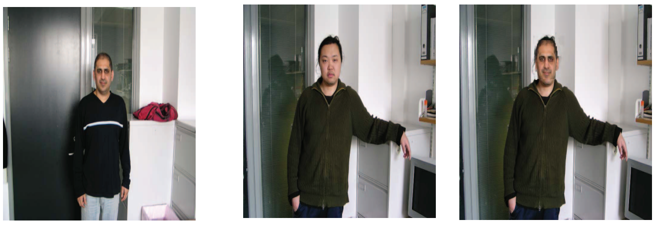

Figure 2. The original image, source image and forged images for the content verification experiments.

We use the normalized cross-correlation as formulated in Equation (4) to measure the similarity between PRNUs (DPRNUs). If the correlation is lower than a threshold, the centre pixel in the window and the corresponding $5\times5$-pixel block centered at the pixel is deemed to be manipulated. As discussed in Chen[6], the cross-correlation follows the Generalized Gaussian (GG) distribution, therefore, we use various thresholds defined as $\mu - c\cdot\sigma$ to analyze the performance of PRNU and DPRNU, where $\mu$ and $\sigma$ are the mean and standard deviation of the correlations distribution, respectively, and *c* in the range from 0 to 3.

Figure 3 demonstrates both schemes can effectively detect the manipulated blocks. But the ROC curve of DPRNU is slightly higher than the ROC curve of PRNU along *y*-axis, indicating a slightly better performance. Nevertheless, at the lower-left corner of Figure 3, the ROC curve of DPRNU is lower than the curve of random guess, when the false positive rate is low. This is because the high threshold leads to both low FP and TP (i.e., the lower-left corner of the figures) so that only a few blocks are detected as manipulated. However, Chen's method [6] is not accurate to small areas, which only contains a few blocks. Therefore, the experimental result is even worse than random guess. This error can be eliminated by using advanced similarity metrics [6]. However, in this work we only concentrate on the evaluation of the PRNU and DPRNU and optimizing integrity verification method is not studied in this paper.

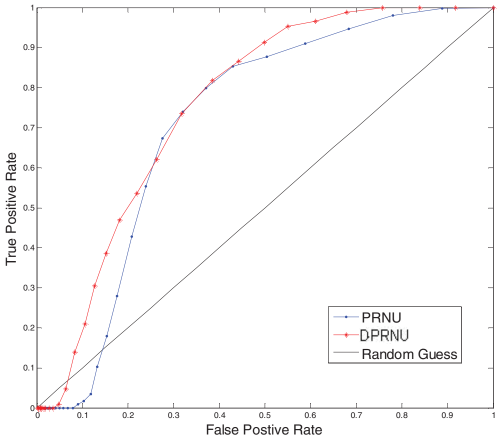

Figure 3. The ROC curve of PRNU and DPRNU in intergrity verification

### C. *Database Optimization*

In the proposed DPRNU method, the fingerprint has been decreased to 1/3 of the original size and thus DPRNU method can save a huge amount of the physical storage space of the fingerprint database. For example, one traditional PRNU fingerprint[1] of a $2048\times1536$ RGB image will cost 68MB on the hard disk, while a DPRNU fingerprint only need 23MB for saving; one PRNU fingerprint of a $640\times480$ RGB image will cost 6MB on the hard disk, while a DPRNU fingerprint only need 2MB for saving. Meanwhile, the DPRNU fingerprint also cost less time for computing. On a Pentium Core II 1.3G CPU and 3 GB Ram computer, computing the similarity between two PRNU fingerprint of two $2048\times1536$ images cost 0.66 second while time consuming of calculating the similarity between DPRNU is 0.23 second. As a result, when using the DPRNU for the fingerprint, the user can save 2/3 of both the physical storage and computing time in setting up and applying the digital library for forensic purposes.

## V. Conclusion

In this paper, we have investigated the forensic method based on PRNU. Due to the interpolation noise, caused by the color interpolation function and tied to the model of cameras, the accuracy of the PRNU-based forensic method has been degraded. Meanwhile, the tremendous physical storage requirement and computation consumption limit the applications of PRNU-based method. Therefore, an innovative DPRNU-based forensic method has been proposed in order to solve the above problems. In the method, the artificial component and physical component are separated according to the CFA and the PRNU are only extracted from the physical component in order to remove the interference caused by the interpolation noise, which increases the accuracy of the camera identification and integrity verification. Meanwhile, due to the separation, the DPRNU are only 1/3 of the size of the traditional PRNU, which saves considerable physical storage in setting up the digital library and fasters the comparison speed between the fingerprints.

Acknowledgement: This paper is supporting by the "Fundamental Research Funds for the Central Universities"

## References

[1] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining Image Origin and Integrity Using Sensor Noise," IEEE Transactions on Information Security and Forensics, vol. 3, no. 1, pp. 74-90, 2008.

[2] A. E. Dirik, H. T. Sencar, and N. Memon, "Digital Single Lens Reflex Camera Identification from Traces of Sensor Dust," IEEE Trans. Information Forensics Security, vol. 3, no. 3, pp. 539–552, Sep. 2008.

[3] J. Fridrich, "Digital image forensics," IEEE Signal Processing Magzine, vol. 26, no. 2, pp. 26-37, 2009.

[4] R. Caldelli, I. Amerini, F. Picchioni and A. De Rosa and F. Uccheddu, "Multimedia Forensic Techniques for Acquisition Device Identification and Digital Image Authentication," in Handbook of Research on Computational Forensics, Digital Crime and Investigation: Methods and Solutions, C.-T. Li (Ed.), Hershey, PA: Information Science Reference (IGI Global), Nov. 2009.

[5] H. Cao and A. C.Kot, "Accurate Detection of Demosaicing Regularity for Digital Image Forensics," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4 , Part: 2, pp. 899 - 910, 2009.

[6] J. Lukas, J. Fridrich, and M. Goljan, "Digital Camera Identification from Sensor Noise," IEEE Transactions on Information Security and Forensics, vol. 1, no. 2, pp. 205-214, 2006

[7] Lukas, J., Fridrich, J., & Goljan, M. "Detecting digital image forgeries using sensor pattern noise." Proceedings of SPIE Electronic Imaging, 6072, 362-372.

[8] A. C. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3948-3959, 2005.